RHCE(Ex-300)on RHEL 7
FullMarks=300
PassMark =210
TIME=3.5hours

**************************** RHCE EXAM ******************************
REDHAT CERTIFIED ENGINEER LINUX CERTIFICATION EXAM
EXAM TIME : 3:30 HRS
PLEASE MAINTAIN THE SILENCE IN EXAM ROOM

===

INSTRUCTIONS
EVERY QUESTIONS IN THIS IS MANDATORY FOR YOU TO COMPLETE

THERE ARE TWO VMS HAS BEEN CONFIGURED IN EXAM.

===

PLEASE Find the below details AND Password for root user is "anaconda"
for both the vm .

VM -I	VM-II
=====	=======
HostName - STATION1.DOMAINX.example.com	HOSTNAME=STATION2.DOMAINX.EXAMPLE.COM
IP - 172.25.X.11	IP= 172.25.X.10
Gateway - 172.25.X.254	GATEWAY=172.25.X.254
DNS-172.25.254.254	DNS=172.25.254.254
Netmask -255.255.255.0	NETMASK=255.255.255.0
Domain :- DOMAINXexample.com	DOMAIN=DOMAINX.EXAMPLE.CO

YOUR CLASSROOM YUM BASEURL http://content.example.com/rhel7.0/x86_64/dvd

Qustion 1 > Set Selinux in Enforcing mode

Set the selinux policy Permissive to Enfrocing on both sides.

Customize the user environment on both systems.

Q-2. Create a custom command called "qstat" on both system1 and system2 that runs the command '/usr/bin/ps -Ao pid,tty,user,fname,rsz'
That command should be available to all users on the system.

Qustion 3 > Configure ssh:

Configure ssh server on serverX.example.com and domain.my113t.org should not have ssh access.

Question 4 | Configure ipv6 in both serverX & desktopX
Configure IPV6 on both serverX.example.com & desktopX.example.com.According to following IP .
serverX.example.com - fddb:fe2a:ab1e::c0a8:X/64
desktopX.example.com - fddb:fe2a:ab1e::c0a8:20+X/64
Note :- ('X' indiacte your System number).

Qustion 5 > Configure Network Teaming.(reaggregation) on both sides.

Configure Network teaming on system1 and system2 use two device called eno1 and eno2
in serverX Ipaddress is 192.168.0.100/24
and desktopX ipaddress is 192.168.0.200/24

Qustion 6 > port forwarding:

Configure PORT FORWARDING incomming connection on port 513/tcp on the firewall to port 132/tcp on network 192.168.0.0/24

Q-7. Configure mail on both system1 and system2.

--> Do not accept incoming mail from external sources.

--> All mail sent locally on this system automatically routed to server1.group11.example.com

--> Mail sent from these systems should show up as comming from group11.example.com

--> Your max test by sending mail to 'another"

--> The system server1.group11.example.com is configured to drop mail for this user http://system1/ received mail.

Qustion 8 > NFS Server:

Export your "/public" directory via NFS to the example.com domain. Make sure that client in example.com domain should able to read only permission in /public.

Configure secure NFS server.

****

Q-9. Export your "/publicshare" directory with using Kerboros via NFS to the example.com domain. Make sure client in example.com domain shoud able to read and write prmission in /publicshare and create a subdirectory called "publicshare" and publicshare directory write. Use keytab for the system1.

http://classroom.exampe.com/pub/keytabs/serverX.keytab

NFS mounts.

****

Q-10. a) Mount /public permanently on the /mnt/secure on the system2.

b) Mount the secure nfs share /publicsecure permanently on the /mnt/securepath on system2

--> Verify that the user ldapuser1 has read and write access on the /mnt/securepath on the system2 and use keytab file

http://classroom.example.com/pub/keytabs/desktopX.keytab

Qustion 11 > Configure SAMBA SHARE:

Q-11. Share the directory "/common" via samba. Your samba server must be a member of "Staff" workgroup.

--> The share name must be "common". Make sure that browsable must be enabled.

--> The shared must be available to example.com clients area.

--> The user "Harry" should have read access to the share with samba

Configure Samba Share.

****

Q-12. Share the directory "/secure" via samba.

--> The share name must be "secure". Make sure that browsable must be enabled.

--> The shared must be available to example.com clients area.

--> The user "rob" should have read access to the share with samba password "animous " and user "robby" shoud have read and write access to the share with samba password "animous"

Multiuser Samba mount.

****

Q-13. Mount /secure the samba share permanentely on the /mnt/secure

--> Mount port on system2 as a multiuser mount.

--> Mount samba share with the credentials of user rob and password "animous"

Qustion 14 > Configure "web server":

Q-14. Configure the system1 as "web server" for the site http://serverX.example.com
--> Download the web page station.html from http://classroom.example.com/pub/updates/station.html
--> Rename the downloaded page as index.html.
--> Copy the index.html file to the "document root" and dont modify

ii) Make sure the web site should be allow to example.com only and deny to my133t.org doimain .

Qustion 15 > Configure "web server":

Create the directory "confidential" for the DocumentRoot of your webserver. Download the page "host.html" from http://classroom.example.com/pub/updates/host.html And move as index.html.It should be accessable to localhost only and not to any other host.

Qustion 16 > Configure name virtual hosting server:

Configure the name virtual hosting server for the site http://wwwX.example.com. Download the page "www.html" from http://classroom.example.com/pub/updates/www.html and rename as index.html under documenRoot "/var/www/virtual". User called rock should able to add some content into /var/www/virtual directory.

Qustion 17 > Configure wsgi web server:

Configure "wsgi" web server site name "webappX.example.com" and download dynamic WSGI conent from http://classroom.example.com/pub/updates/webpp.wsgi and stored inside virtual web server DocumentRoot of your webserver. and donot effect virtual web serevr. port should be 8999 and client should access the web site using webappX.example.com:8999.

17: confiure ssl web server

Configure secure web server site name http://serverX.example.com ant the web site will nedd to protect with tls. and the certificate can be download from http://classroom.example.com/pub/example-ca.crt http://classroom.example.com/pub/tls/private/server11.key http://classroom.example.com/pub/tls/private/server11.crt

Qustion 19 > CONFIGURE "target server":

configure target server use the this iqn iqn.2015-02.com.example.group11:system1 and 3G backing store device volume group name iscsi_storage. iscsi storage should availabe to desktopX.example.com sysetm only.

20: Configure iscsi client.

Create a new 2024Mb iscsi target on your desktopX.example.com machine. this target should be called iqn.2014-09.com.example.group11:system1 and assign file system ext4 and mount under /mnt/iscsi directory.

Qustion 21 > Configure mariadb.

Install mariadb database and user root password is animous database sholud access only localhost. create a "Contacts" datebase and restore a data base backup http://classroom.example.com/pub/updates/mariadb.dump. rob user can query and access "contacts" database should be use password is "animous".

Qustion 22 >list the users information who have the password=animous from user table .user table located in mysql database. and store the result in the file name password.txt in the location /mnt

Qustion 23 > Script:

Write the script called /root/script. If you pass an argument as "redhat" it should print "fedora" . If you pass an argument as "fedora" it should print "redhat". If won't pass any argument (or) if you pass another argument other than "redhat" and "fedora"it will print standard error "/root/script redhat|fedora".

Q-24. Create a script on system1.

--> It should be a single argument which is the name of file that contain usernames.
--> If argument is not supplied it should display usage :/root/batchusers and exit.
--> If non existant file is specified, it should display file not found.
--> Accounts should be encounted with login shell /bin/false
--> Script does not root need to set password.