

Vendor: RedHat

Exam Code: RHCE-CN

Exam Name: Red Hat Certified Engineer — RHCE

Version: Demo

Exam Times:

RHCE: Two hours.

Pass Scores:

Total 300 points. Pass at 210 points.

Exam Environment:

Take examinations on a real system with a pre-installed virtual machine.

All exams must be completed in the virtual machine.

Network must be well configured. If the network cannot be accessed, you will not pass the exam.

In the iptables configuration, if you need to refuse the access, please use "Reject". (The default is set as ACCEPT.)

Note:

Your IP address, Host Name, Gateway and DNS has been configured.

IP address: 172.24.30.5/24

Hostname: station.domain30.example.com

vim /etc/hosts

172.24.30.5 station.domain30.example.com

Add the corresponding relation between the host name and IP in the hosts records.

You are a member of the domain30.example.com host domain, another domain is t3gg.com---172.25.0.0/16 network.

QUESTION 1

To ensure SELinux open after the boot:

Answer:

```
vim /etc/sysconfig/selinux
selinux=enforcing
setenforce 1
getenforce
```

QUESTION 2

Open system kernel forwarding packets function:

Answer:

```
vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
sysctl -w (Effective immediately)
```

The following commands should be executed without sysctl.conf option:

```
sysctl -a |grep net.ipv4
sysctl -P net.ipv4.ip_forward = 1
sysctl -w
```

QUESTION 3

Configure SSH access as follows:

- Harry has remote SSH access to your machine from within example.com
- Clients within t3gg.com should NOT have access to ssh on your system

Answer:

```
yum install -y sshd
chkconfig sshd on
vim /etc/hosts.deny
sshd: 172.25.0.0/16
```

Use iptables:

```
iptables -F
iptables -X
iptables -Z
iptables -nvL
iptables -A INPUT -s 172.25.0.0/16 -p tcp -dport 22 -j REJECT
services iptables save
```

Each finished writing a iptables rules saved

iptables -nVL

cat / etc / services can be used to view port

If wrong, can be modified in vim / etc / sysconfig / iptables

QUESTION 4

Configure FTP access as follows:

- Download from catalog: / var / ftp / pub using anonymous is allowed
- Clients within t3gg.com should NOT have access to FTP on your system

Answer:

```
yum install -y vsftpd
```

```
chkconfig vsftpd on
```

```
services vsftpd start
```

Deny: uninstall hosts.deny or use iptables

```
vim /etc/hosts.deny
```

```
vsftpd: 172.25.0.0/16
```

```
iptables -A INPUT -s 172.25.0.0/16 -p tcp -dport 20:21 -j REJECT
```

```
services iptables save
```

QUESTION 5

Mount /root/cdrom.iso under /opt/data, and take effect automatically at boot-start

Answer:

```
cd /opt/
```

```
mkdir data
```

```
mount -t iso9660 -o loop /root/cdrom.iso /opt/data
```

```
vim /etc/fstab
```

```
/root/cdrom.iso /opt/data iso9660 defaults,loop 0 0
```

QUESTION 6

Configure Web server as follow:

Clients within http://station.domain30.example.com should have access to Web server on your system

Answer:

```
yum install -y httpd
```

```
chkconfig httpd on
```

```
cd /etc/httpd/conf/
```

```
vim httpd.conf
```

```
NameVirtualHost 172.24.30.5:80
```

```
<VirtualHost 172.24.30.5:80>
DocumentRoot /var/www/html/
ServerName tation.domain30.example.com
</VirtualHost>
service httpd restart
```

QUESTION 7

Build a web server to enable the virtual host. So `http://www.domain30.example.com` able to access to the page `/www/virtual` directory, download from `http://ip/dir/example.html`. And ensure, `http://station.domain30.example.com` also be access to the contents of.

Answer:

```
mkdir -p /www/virtual
cd /www/virtual
wget http://ip/dir/example.com
cp example.com index.html
se manage fcontext -a -t httpd_sys_content_t '/www(/.*)?'
restorecon -vRF /www
vim /etc/httpd/conf/httpd.conf (Create a new host)
<VirtualHost 172.24.30.5:80>
DocumentRoot /www/virtual/
ServerName www.domain30.example.com
</VirtualHost>
service httpd restart
```

Verify with elinks

Other kinds of questions:

Download files from `http://ip/dir/restircted.html`. Local user have access to it through `http://dtop30.dn.ws.com/restircted`, but Clients within `remote.com` should NOT have access to it.

```
htpasswd -cm /etc/httpd/.htpasswd sisi
htpasswd -m /etc/httpd/.htpasswd tami
<VirtualHost 172.24.30.5:80>
DocumentRoot /www/virtual/
ServerName www.domain30.example.com
<Directory "/www/virtual/">
AuthName "www.domain30.example.com"
AuthType basic
AuthUserFile /etc/httpd/.htpasswd
Require valid-user
</Directory>
```

```
</VirtualHost>  
services httpd restart
```

QUESTION 8

Download files from <http://ip/dir/restricted.html>. Local users have access to it through <http://station.domain30.example.com/restricted>, but Clients within t3gg.com should NOT have access to it.

Answer:

```
cd /var/www/html  
wget http://ip/dir/restricted.htm  
iptables -A INPUT -s 172.25.0.0/16 -p tcp -dport 80 -j REJECT  
service iptables save
```

QUESTION 9

Configure NFS server to share /common directory with domain30.example.com. Authenticate the clients devices have the access to it as root user.

Answer:

```
yum install -y nfs  
chkconfig nfs on  
chkconfig rpcbind on  
vim /etc/exports  
/common 172.24.30.0/255.255.255.0 (rw,no_root_squash)  
showmount -e 172.16.30.5  
mount -t nfs 172.16.30.5:/common /mnt
```

QUESTION 10

Configuring samba server, shared / common, and can browse to the. User harry shared read-only, if necessary, harry users password for harryuser were.

Answer:

```
yum install -y postfix  
chkconfig smb on  
useradd harry  
smbpasswd -a harry  
vim /etc/samba/smb.conf  
[common]  
comment = common  
path = /common  
browseable = yes
```

```
read only = yes
testarpm
getsebool -a |grep samba_share_nfs
setsebool -P samba_share_nfs=1
services smb restart
mount -t cifs //172.16.30.5/common /mnt -o username=harry%harryuser
```

QUESTION 11

Configure an email server domain30.example.com, and it requests to send and receive emails from the local server or the user harry can send or receive emails from network. The email of user harry is /var/spool/mail/harry. Please note: the DNS server has already been MX record.

Answer:

```
yum install -y postfix
chkconfig postfix on
vim /etc/postfix/main.cf
inet_interfaces = all
mydestination = example.com, domain30.example.com, localhost
mynetworks = 172.16.30.0/24, 127.0.0.1/8
services postfix restart
```

Test:

```
netstat -tulnp |grep 25
hostname
echo hello |mail -s "test"root@example.com
cat /var/spool/mail/harry
```

QUESTION 12

Connect to mail server and send email to admin, ensure that user harry can revive it.

Answer:

```
vim /etc/aliases
admin: harry
newaliases
```

QUESTION 13

Configure Kernel parameters rhelblq=1 and enable /proc/cmdline to verify your Kernel parameters.

Answer:

Vim /etc/grub.conf

Write the end of the kernel line

To see after restart

cat /proc/cmdline

QUESTION 14

Configure cron as follow:

Clients tom should NOT have access to cron

Answer:

useradd tom

vim /etc/cron.deny

tom

Effective immediately save and exit.

QUESTION 15

Write a script / root / program, the requirements when the input parameter kernel to the script, the script returns the user, the input parameters to the script user, the script returns the kernel. While the script no parameters or parameter error, the output from the standard error output usage: / root / the program kernel | user

Answer:

vim /root/program

```
#!/bin/bash
```

```
if [ "$1" == "kernel"];then
```

```
echo "user"
```

```
elif ["$1" == "user"];then
```

```
echo "kernel"
```

```
else
```

```
echo "usage:/root/program kernel|user"
```

```
fi
```

Test:

```
chmod a+x /root/program
```

```
./root/program kernel
```

```
./root/program user
```

```
./root/program lll
```

QUESTION 16

Please visit iscsi shared storage, storage server address is 172.24.30.100, ceded 1500M space, formatted with the ext3 file system, mount / mnt / data, and boot

automatically mount.

Answer:

```
yum install -y iscsi*
chkconfig iscsid on
chkconfig iscsi on
iscsiadm -m discovery -t st -p 172.24.30.100:3260
iscsiadm -m node -T iqn.2011 -p 172.24.30.100 -|
service iscsi restart
fdisk -|
fdisk /dev/sda
partx -a /dev/sda
partx -a /dev/sda
mkfs.ext3 /dev/sad1
yum -y install tree
cd /var/lib/iscsi
tree . view iqn
cd /mnt
mkdir data
blkid /dev/sda1 (View UUID, UUID mount)
vim /etc/fstab
UUID=XXX /mnt/data ext3 default, _netdev 0 0
mount -a
```

QUESTION 17

Configuring the NFS service that will /mnt /storage directory with read-only shared to the example.com domain user when the client as the root user will also have access to the root directory permissions to read-only shared to cracker.org domain users.

Answer:

```
# vim /etc/exports
/mnt/storage *.example.com(ro, sync, no_root_squash)
/mnt/storage *.cracker.org(ro, sync)
```

QUESTION 18

Example.com only allows access to the local SSH.

Answer:

```
# vim /etc/hosts.allow
sshd: .example.com
# vim /etc/hosts.deny
```

sshd: ALL

QUESTION 19

Samba configuration requirements are as follows:

1. The Working Group called RHCE
2. Types of user authentication
3. Shared / mnt / storage directory share name for the share
4. The shared directory allows user1 and user2 user has write permissions to other users are read-only, if you need password are redhat
5. only allows the user to access the shared directory domain example.com

Answer:

```
# yum install -y samba
# vim /etc/samba/smb.conf
[global]
workgroup = RHCE
security = user
[share]
path = /mnt/storage
write list = user1 user2
hosts allow = .example.com
# ( echo redhat ; echo redhat ) | smbpasswd -s -a user1
# ( echo redhat ; echo redhat ) | smbpasswd -s -a user2
# service smb start; chkconfig smb on
```

QUESTION 20

Establish vsftpd server, so that only allow user1 user access, and cannot jump out of home directories only allow users to upload and download example domain, allowing only example domains can be accessed.

Answer:

```
# yum -y install vsftpd
# vim /etc/vsftpd/vsftpd.conf
userlist_deny=NO
userlist_file=/etc/vsftpd/vsftpd.user_list
chroot_list_enable=YES
chroot_list_file= /etc/vsftpd/vsftpd.chroot_list
anon_upload_enable=YES
anonymous_enable=YES
# mkdir -p /var/ftp/incoming; chmod 777 /var/ftp/incoming
# chcon -t public_content_rw_t /var/ftp/incoming
```

```
# setsebool -P allow_ftp_anon_write 1
# setsebool -P ftp_home_dir 1
# vim /etc/vsftpd/vsftpd.user_list
user1
# vim /etc/vsftpd/vsftpd.chroot_list
user1
# service vsftpd start; chkconfig vsftpd on
# vim /etc/hosts.deny
vsftpd: ALL EXCEPT .example.com
```

QUESTION 21

Create new mail server, the following:

1. Allow localhost and remote hosts can access
2. Allow example.com users can relay to refuse remote test
3. All mail sent to the user3 will be sent to user2
4. Confirm / var/spool/mail/user1 exist
5. Example.com domain only allows the user to receive mail via pop3

Answer:

```
# yum install postfix -y
# alternatives --set mta (Choose postfix)
# service sendmail stop; chkconfig sendmail off
# cd /etc/postfix
# vim main.cf
myhostname = stationX.example.com
mynetworks_style = subnet
mydestination = $ myhostname
myorigin = $ myhostname
relay_domains = example.com, $mydestination
inet_interfaces = all
smtpd_client_restrictions =
check_client_access hash:/etc/postfix/access,
check_sender_access hash:/etc/postfix/access,
check_recipient_access hash:/etc/postfix/access,
permit_auth_destination,
permit_mynetworks,
# vim /etc/postfix/access
remote.test REJECT
# vim /etc/aliases
user3: user2
# postalias /etc/aliases
# postmap hash:/etc/postfix/access
```

```
# touch /var/spool/mail/user1 (Generally exist by default)
# chown user1:mail /var/spool/mail/user1
# chcon --reference=/var/spool/mail/root /var/spool/mail/user1
# chmod 660 /var/spool/mail/user1
# Reject remote.test domains can use iptables.
# iptables -A INPUT -p tcp --dport 25 -s remote.test(Written IP network segment) -j
REJECT
# service postfix start; chkconfig postfix on
# yum install dovecot
# vim /etc/dovecot.conf
protocols = pop3
# service dovecot start; chkconfig dovecot on
# iptables -A INPUT -p tcp --dport 110 -s 192.168.0.0/24 -j
ACCEPT
# iptables -A INPUT -p tcp --dport 110 -j REJECT
# service iptables save; chkconfig iptables on
```

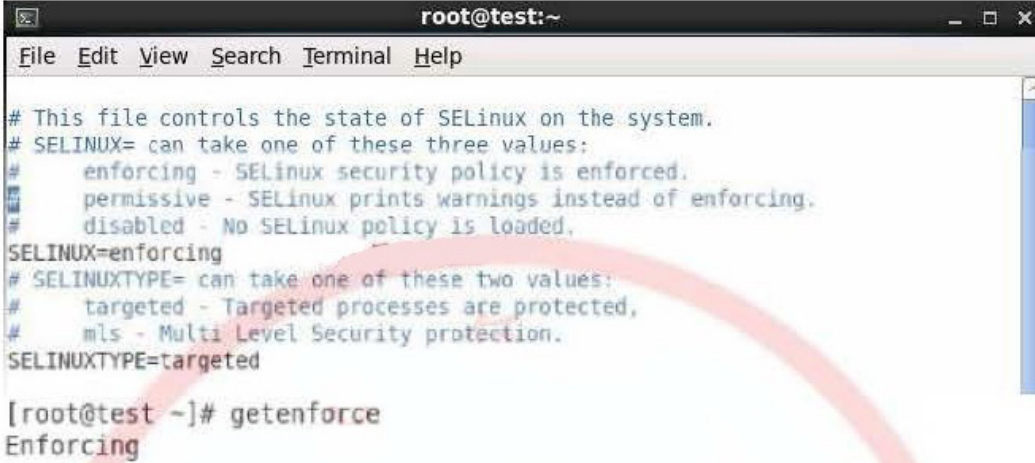
www.Pass4itSure.com

Laboratory Manual

Lab 1

Configure Selinux it should be in enforcing mode.

```
[root@test ~]# vim /etc/selinux/config
```



The screenshot shows a terminal window titled "root@test:~" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content displays the configuration of SELinux in the file /etc/selinux/config. The configuration is as follows:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Below the configuration, the command `getenforce` is executed, resulting in the output `Enforcing`.

www.Pass4it

Lab 2

Turn on your kernel to forward packets function.

```
[root@test ~]# vim /etc/sysctl.conf
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1

[root@test command]# cat /proc/sys/net/ipv4/ip_forward
1
```

www.Pass4itSure.com

Lab 3

The existing two network segments, example.com for 172.16.0.0/16, crake.com for 172.25.0.0/16, hereby request that the example.com network segment to access the machine cannot access, crake.com segment.

```
[root@test ~]# iptables -F
[root@test ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

[root@test ~]# iptables -A INPUT -s 172.25.0.0/16 -j REJECT
[root@test ~]# /etc/init.d/ip
iptables iptables
[root@test ~]# /etc/init.d/iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@test ~]# /etc/init.d/iptables restart
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: mangle nat filte[ OK ]
iptables: Unloading modules: [ OK ]
iptables: Applying firewall rules: [ OK ]
[root@test ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
REJECT    all  --  172.25.0.0/16         anywhere             reject-with icmp-po
rt-unreachable ✓

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

WWW.P

Lab 4

Configure the ftp server, anonymous users can upload and download, reject the 172.25.0.0/26 network segment.

```
[root@test ~]# yum install *ftp*
Loaded plugins: refresh-packagekit, rhnplugin
This system is not registered with RHN.
RHN support will be disabled.
Setting up Install Process
Package report plugin-ftp 0.18-7.el6.i686 already installed and latest version
Package report-config-ftp-0.18-7.el6.i686 already installed and latest version
Package gvfs-obexftp-1.4.3-9.el6.i686 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package ftp.i686 0:0.17-51.1.el6 set to be updated
```

www.Pass4itSure.com