Instructions:

- In VirtualBox create a NAT network called ***"LFCS Practice Exam Network"*** and configure it to use the subnet ***192.168.5.0/24***
- In VirtualBox configure each individual vm to use this network. The vms are already assigned static IPs but still need to be configured in VirtualBox to use the NAT network listed above.
- Perform all actions on **home-1** unless asked to ssh into another server. Always return to **home-1** after completing tasks on other servers.
- The username is **root** and the password is **redhat**
- The following programs are installed for your convenience and they are not guaranteed to be automatically installed on the exam and in general as of this writing they are not installed by default on CentOS 7. But it has been reported that there is not much you should have to install on the exam.

Program Name	Package Name
lsof	lsof
tree	tree
elinks	elinks
dig	bind-utils
nslookup	bind-utils
route	net-tools
netstat	net-tools
semanage	policycoreutils-python
traceroute	traceroute

1.	Managing process limits is an important part of a Linux admins job. a. Make it so that the group *engineers* can only run a max of 10 process at a time. Create soft and hard limits for this. b. Also make it so the user *eric* (who also happens to be in the *engineers* group) is not subject to these restrictions. *Eric* should be able to run an unlimited number of processes similar to the root user.
2.	Change the hostname of the system to *home-1.lfcs-practice.com* and make it resolve to 127.0.0.1
3.	There is a service called *chronyd* currently running on *home-1* a. Identify the port number that this service is using and write it to the file */root/service_port.txt* b. *Identify which files this service is writing to and add the names of those files to */root/service_files.txt*

4	Identifying and setting the run level of a machine is an important task. a. Find the current runlevel of the machine *home-1* and write it to the file */root/runlevel.txt* b. Set *home-1* to persistently boot into run runlevel 5 (graphical.target)
5	a. Go to the /root/unique/dir1 directory and find the one file that is different. Save the file name to /root/unique_file.txt. b. Find the files in /root/unique/dir1 that are not in /root/unique/dir2.
6	Parsing files is an extremely useful skill set to have as a Linux admin is always tracking down issues. a. Find all lines in the file /var/log/secure that contain the string "*FAILED*" followed by the string "*linda*" and save the output to a file named */root/search/6/securefile.txt* b. Find all files in */var/log* that contain the string "Erased" and copy them to the directory */root/search/6/erased* c. Find all lines that start with the string "name" in the file /proc/crypto and save the output to */root/search/6/crypto.txt*
7	Often as linux administrator you will have to make tar archives. a. Create a compressed tar archive of the /etc directory called *etc_backup.tar.bz2* (*make sure to to use the bzip2 compression algorithm*) - store this backup in the directory */root/backups/7*
8	Create and Manage Hard and Soft Links a. Create a hard link named *routines_hard.sh* in /root/opt/vbox/links that points to */opt/VBoxGuestAdditions-5.2.20/routines.sh* b. Create a soft link named *license_soft* in */root/opt/vbox/links* that points to */opt/VBoxGuestAdditions-5.2.20/LICENSE* c. Remove the link */root/opt/vbox/links/uninstall.sh*.
9	Copying files is an important part of a Linux admins job. Use the appropriate tools to complete the following tasks. a. Find all files and directories in /etc that start with "a" or "b" and copy them to the directory */root/found/8/permissions* while preserving their permissions. b. Find all files in /etc that are greater than 1MB and save their absolute paths to the file */root/found/8/big-files.txt* c. Find all files in /etc not owned by root and copy the files to */root/other_users*

10	Extract the */root/backups/7/etc_backup.tar.bz2* archive into the directory */root/backups/7/restored*
11	ssh to ***server-1*** and create a virtual host called *server1.lfcs-practice.com* with a document root of */web/html*. Make sure that this new virtual host does not interfere with the main server configuration called *lfcs-practice.com*. When you are done with this exercise be sure to come back to **home-1**
12	As a Linux administrator you will often have to create new users and groups. Create the following users with the following details - If the supplemental groups listed do not exist, create them. a. bob - Supplemental Group engineers - PW: cent6 b. tim - Supplemental Group webdev - PW: cent6 c. ben - Supplemental Group chemical - PW: cent6 d. All accounts created must expire one year from today. e. Set the user bob's default shell to zsh f. Set the user tim's default home directory to /shadow-soft - if this directory does not exist, create. Apply the same SELinux contexts and permissions to /shadow-soft that would be found on a user's /home directory such that Tim and only Tim will have access to /shadow-soft
13	Managing user access is an import part of a Linux admin jobs. a. Give the user *ben* complete Sudo access to the machine. Make sure they don't need to use their password to run commands as root. b. Give the user *tim* sudo access to the iptables tool
14	ssh to ***server-1*** *and c*onfigure the firewall to allow tcp traffic on port 3306 from ip address range 192.168.5.0/24 - make sure to add this rule as the second rule in the chain and make it persistent after a reboot or restart of iptables.
15	ssh into ***server-1*** and add a static route to 198.49.23.145 by way of 192.168.5.130 (server2). Go back to ***home-1*** after you are done.
16	Make user *bob's* password expired so he will be forced to change it upon his next login
17	Create and Manage RAID Devices a. Use partitions */dev/sdb1 and /dev/sdc1* to create a raid 1 device named */dev/md0* b. Format the */dev/md0* device with an *ext4* file system and make sure it is persistently mounted on */mnt/raid* c. Next add the partition */dev/sdd1* to the raid array.

18	File Systems and Swap a. Use the 2GB disk located at */dev/sdd2* to add to the current swap device. Use the entire disk. Make sure it is active upon reboot b. Use the 512MB disk partition located at /dev/sdd4 to make an ext4 file system and create a label for it called “data-1” c. Use the 512MB disk partition located at /dev/sdd5 and format it is an xfs file system. Label it “data-2”
19	Create and Manage Containers. Ssh into **server-2** and do the following: a. Remove the docker container “nginx_container” b. Create a new docker container named “apache_container” with the latest image of http c. Enable the container to start when the docker service starts (on boot)
20	Virtual Machines ssh over port 60022 to **scriptbabies.com** using your first name and the password (**redhat).** You will have a vm on that host labeled with your name (eg. *marco_vm, niyi_vm, jonathan_vm etc.*). a. Check if your vm is running or not. If it’s not running start it up. If it’s already running then shut it down and then start it back up. b. Also set the vm to autostart when the host starts. c. Increase your vm’s memory to 1024MB You are welcome to practice starting, stopping, setting autostart, disabling autostart and listing the vms as much as you like. Return to **home-1**
21	Scripting a. Make a script file named *backup.sh* located in /scripts for the user linda to run where she is creating a backup named backup.tar.gz of /home/linda in *gzip* format. Also print a message saying “All done” at the end of the backup. The script should be creating the backup in the same directory where the script is located (/scripts). b. Add the appropriate permissions and test the script
22	On **home-1** repair the disk */dev/sdd3*. The disk is not mounted.
23	Search for files a. Find all files in */usr* that are greater than 4Mb and print their absolute paths to the file */root/found/23/big-files.txt* b. Find all files *and* directories in */run* that do **not** belong to the user *root* and print their absolute paths to the file */root/found/23/not_root.txt*

	c. Find all files in /usr/bin that have the SUID bit set and copy the files to /root/found/23/suid d. Find all files in /usr/bin that have the GUID bit set and copy the files to /root/found/23/guid
24	Scheduling tasks to run at a certain time and date a. Make the user linda to perform a xz compressed backup of her /home/linda/Documents and shutdown her computer afterwards of at 2:00AM on every Saturday for the month of June. The backup should be saved in */home/linda/backups/24/documents.tar.xz* b. Make the user linda perform a **non** compressed backup of /opt/VBoxGuestAdditions-5.2.20 at the top of every hour everyday. The backup should be saved in /home/linda/backups/24/vbox.tar
25	Perform the following tasks on **home-1** a. There is a NFS share on **server-1**. Mount this share persistently on top of the directory /nfs b. There is a Samba Share on **server-1**. Mount this share persistently on top of the directory /samba (you can connect as the user ***student*** with password: ***redhat***) or as the user ***guest*** without a password.
26	Perform the following tasks on **home-1**: a. Redirect STDOUT of the following command to a file named /root/redirect/stdout.txt **grep sshd /etc/*** b. Redirect STDERR of the following command to a file named /root/redirect/stderr.txt **grep sshd /etc/*** c. Redirect STDOUT and STDERR of the following command to a file named /root/redirect/stdout_and_stderr.txt **grep sshd /etc/***
27	Delete the file */root/impossible.txt*
28	Do the following procedures on **server-2**: a. Allow for linda to remotely login without using her password b. Allow only ben to ssh into server-2 using a password c. Set the log level for ssh to DEBUG d. Disable X11 forwarding

29	The user eric has had some bad login attempts on **home-1**. Using the log files, find the lines that pertain to eric's bad login attempts and save them to */root/bad_login.txt*
30	ssh to ***server-1*** *and c*onfigure the firewall to allow tcp traffic on port 80 from ip address range 192.168.5.0/24 - makes sure to add this rule as the first rule in the chain and make it persistent after a reboot or restart of iptables. Go back to ***home-1*** after you are done.
31	Perform the following tasks on **home-1**: a. Find all lines in /usr/share/dict/book that begin with "Algernon" and save to the file /root/found/22/algernon.txt b. Find all lines in /usr/share/dict/book that start with "Jack" and end with "are" and save to the file /root/found/22/jack.txt c. Find all lines in /usr/share/dict/book that start with "this" or "That" regardless of case and save to the file /root/found/22/this_or_that.txt