S1 Root-tar-n of the Jedi (10 points)

Define/Explain the following terms. (2 points each)

1. root

super user, can do anything, should not log in directly

2. Zombie process

Child process after completing and exiting control to parent. But has not been cleaned up yet,

3. Hard link

Additional reference to a file. Must be on same system. Points directly to the file itself.

4. Soft link

Additional reference to a file or folder. Like a shortcut. Can be on a different system. Links to a file that points to the original file or folder.

5. tar

compression for archiving and security

S2 The Internet Strikes Back (15 points)

For each of the connection descriptions below, do the following:

1. Create a static connection for device eth0 with the IPv4 address, gateway, and name given.
2. Add the DNS given.
3. Activate the connection.
4. Check to be certain the connection is active.
5. Add the secondary IP address to the connection by
   a. Editing the configuration file
   b. Using a single command
6. If a connection is not possible, indicate the reason why.

Connection	**1**	**2**
Name	final-eth0	exam-eth0
IPv4	192.168.11.10/16	192.168.199.10/24
Gateway	192.168.12.1	192.168.12.1
DNS	192.168.0.254	192.168.0.254
Secondary	10.20.30.40/24	10.20.30.40/16

1. (3)
```
nmcli con add con-name “final-eth0” ifname eth0 type ethernet ip4 192.168.11.10/16 gw4 192.168.12.1
```
2. (2)
```
nmcli con mod “final-eth0” ipv4.dns 192.168.0.254
```
3. (2)
```
nmcli con up “final-eth0”
```
4. (2)
```
nmcli con show --active
```
5.
   a. (2)
```
nmcli con mod “final-eth0” +ipv4.addresses 10.20.30.40/24
```
   b. (2)
```
echo “IPADDR1=10.20.30.40” >> /etc/sysconfig/network-scripts/ifcfg-eth0
  echo “PREFIX1=24” >> /etc/sysconfig/network-scripts/ifcfg-eth0
```
6. (2) exam-eth0 not possible because Gateway is not on the same subnet as the IP address

S3 Access of the Clones (20 points)

Using commands, perform the following:

1. Create 2 Users with the given username password combination
   a. Username: {your first initial} + {your surname} pass: F1n@lEx@m
   b. Username {your first name} + {initial letter of your surname} pass: f!nal3xam
2. Create a new group called exam and add both users to the group
3. Switch to the first new user you created in that user’s home directory
4. Change the permissions on the Documents directory to allow others to write
5. In the user’s Documents directory using a single command create a file called “file1.txt” that has the text “This is a test file”
6. Switch to the other new user but stay in the first user’s Documents directory
7. Temporarily change the default permissions for new files to be the following:
   a. Owner - write only, Group - read only, Other - none
8. With a single command create a file named “file2.txt” with the same text as file1.txt
9. Switch to root and change the group for both files to exam

1. (2)
   a. `useradd jledet` (and either the passwd command or some other acceptable method)
   b. `useradd josephl` (and either the passwd command or some other acceptable method)

```
2. (2) groupadd exam
   usermod –aG exam jledet
   usermod –aG exam josephl
3. (1) su - jledet
4. (2) chmod o+w Documents
5. (2) echo “This is a test file” > Documents/file1.txt
6. (1) su josephl
7. (2) umask 0537
8. (2) cat file1.txt > file2.txt
9. (2) su
   chown :exam file1.txt
   chown :exam file2.txt
```

If you were to run the ls –l command, what would be displayed (i.e. permissions and ownership)? And fill in the grid below based on the information gained.

(2)

```
-rw-rw-r--     jledet        exam file1.txt
--w-r-----     josephl       exam file2.txt
```

(2)

	User1 can read	User 1 can write	User 2 can read	User 2 can write
file1.txt	Y	Y	Y	Y
file2.txt	Y	N	N	Y

S4 Revenge of the Soft Link (15 points)

1. Create a hard link to the file file1.txt you created in the previous section. This hard link should be named user1file1.txt and be placed in user2's Documents directory.

(3) `ln /home/jledet/Documents/file1.txt /home/josephl/Documents/user1file1.txt`

2. How would you verify that the hard link was created?

(2)`ls –l` should show 2 for how many links are there

3. Create a soft link to the file file1.txt you created in S2. This soft link should be named user1file1.txt and be placed in user1's Desktop directory.

(3) `ln -s /home/jledet/Documents/file1.txt /home/jledet/Desktop/user1file1.txt`

4. How would you verify that the soft link was created?

(2) `ls –l` on Desktop should show `user1file1.txt -> /home/jledet/Documents/file1.txt`

5. Run a command to delete the original file.

(2) `rm file1.txt`

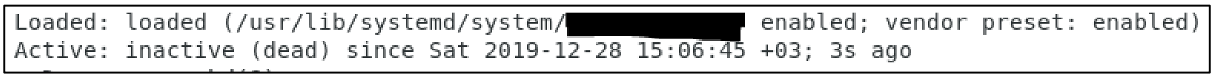
6. What happens to the hard and soft links you created?

(3) File still exists. Hard link still accesses file. Soft link is hanging.

S5 The Service Awakens (20 points)

1. Write the command to show the current status of the sshd service. When you do, you see the below information.

(4) `systemctl status sshd.service`



```
Loaded: loaded (/usr/lib/systemd/system/[redacted] enabled; vendor preset: enabled)
Active: inactive (dead) since Sat 2019-12-28 15:06:45 +03; 3s ago
```

2. What can you understand from this information?

(4) It is stopped (inactive) and enabled.

3. Describe two (2) possible scenarios for how the sshd service came to be in this state.
   a. (4) It was started at system startup, but stopped since then
   b. (4) It was disabled at startup but enabled since then.

4. You will need the sshd service in the next section so write the command to change the service to a running state.

(4) `systemctl start sshd.service`

S6 The Rise of SSH (20 points)

We want to be able to log in to a remote server (named remserver) without using passwords.

1. What is the name of the software and command we would use to log in to a remote server?

   (3) Secure Shell (ssh)

2. Write the command(s) to set up remote access without the need for passwords.

(3)
```
ssh-keygen
ssh-copy-id remserver
```

3. How would we remove the access to login as root on the remote server.

(3) Edit the sshd_config file to have PermitRootLogin to no

4. If you try to log in as root from a different computer, what message will you receive?

(3) Incorrect password multiple times

5. Why do we receive this message?

(4) So that hackers do not know that we disallowed root access.

6. As we saw in class, even though root login is not allowed, it is still possible to gain root access from our desktop to the remote server. What steps do we need to follow to achieve this (without changing any of the settings we changed in this problem)?

(4) Login using ssh to the remote server as a registered user. Then su into root.