Assessment 4.

1. A user account is a location on a computer network server used to store a computer username, password and other information. I allows or does not allow a user to connect to a network or another computer.
2. The user’s shell is the user’s command line interpreter. It interprets the commands the user types and and arranges for them to be carried out.
3. The users home directory or login directory in a unix Os, is the repository for the user’s personal files.It is also the directory that a user a user is first in, after logging into the system.
4. # useradd manolo -u 33545
5. # groupadd sysmgrs
6. # useradd sarah -g sysmgrs
7. # useradd natasha -s /sbin/login
8. rwx rw- rx-
9. Ls -l
10. # chown <ownername> <newowner>
11. # chgrp <groupname> <filename>
12. Soft or symbolic link is a shortcut to a file or a directory.
13. Soft link is a short cut to a file or a directory/ hard link is a clone to a file or a directory. Soft link recognized by an arrow → /hard link recognized bu an inode. Soft link can span file system/hard link does not span file system.
14. a. Ask them to use soft or hard link to have access to the same file or directory which can accessed without getting into each others directory.

b. # ln -s /home/ceo/project1 /home./jsmith/project2. or for hard link #ln /home/ceo/project1 /home jsmith/project2

1. # chmod <filename>
2. Aninode is a file’s id in a server, and it is using that id to manipulate the server.
3. # ls -li
4. # cat /etc/profile
5. Ssh, secure socket shell is a network protocol that provides administrators with a secure way to access a remote computer.
6. Ssl, secure socket layer, is a standard technology for establishing an encrypted link between a web server and a browser.
7. Putty is considered a secure shell because it is run on the ssh daemon protocol connection to access remote servers.
8. Selinux is Security enhanced Linux is a linux kernel security module that provides a mechanism for supporting access control security policies, keeping everything in the server exactly where they are supposed to be.
9. The browser makes a query to the DNS and the DNS gets the IP address, and use that address to request the url page from the server. The server will receive the response, manipulate the request and send the response back to the browser allowing the client to open the page.
10. 3 way handshake is method used in a TCP/IP network to create a connection between a local host and server. The host establishes a request from the server and the server acknowledges that request before the final request is made.
11. The boot up process in linux is made of 6 layers the BIOS performs system checks on all the hardware components initiates and execute the master boot loader located in the first sector of the disk, and carrying information of the Grub boot loader. The grub displays a flash screen and and loads and execute kernel and initrd images.. The kernel mounts the root files as specified in the grub.conf file, looks up at the /etc/inittab file to decide the linux run level usually in by the system admin by default.
12. To update the Os version check the old version using # uname -r, then update using # yum update -y.
13. To harden or secure a server is to tighten it vulnerability to security breach. You can do that by setting up root password on run level 1, in the vi /etc/sysconfig/init file, changing from /sbin/sushell to SINGLE=/sbin/sulogin. Set and encrypted password by # vi /boot/grub.grub.conf file and pasting the encrypted file after the hidden menu, set selinux into enforcing mode in the # vi /etc/selinux/config, setting a strong password policy by # vi /etc//login.defs, managing users in the active directory and patching the server using # yum update -y.