SECTION 3:

First Login ROOT user

Change the root user's password if not root enforced by your host:

```
passwd
```

Change Prompt Appearance:

```
cd /etc

vi bashrc
```

Comment default line:

```
# [ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\u@\h \w]\\$ "
```

Add the following underneath commented line:

```
PS1='\u@\H:\w\$ '
```

Add new user to server:

```
adduser username
```

Give new user a password:

```
password username
```

Give new user root privileges:

```
visudo
```

Prevent root user login – edit sshd_config file – make a backup copy of file

```
cd /etc/ssh

cp sshd_config sshd_config.bak

vi sshd_config
```

Restart the sshd service

```
systemctl restart sshd
```

Logout of server and login as non root user you created:

```
exit
```

First Login NON ROOT User

Update the packages:

```
sudo yum update
```

Install Nano

```
sudo yum install nano
```

Create .ssh directory in your user's home directory:

```
cd

mkdir .ssh/
```

Logout to generate SSH keys

```
exit
```

SSH Key Authentication – Commands Typed Locally

Generate Keys

```
ssh-keygen -t rsa -b 4096
```

Copy public key to server:

```
scp .ssh/public_key_name user@ip:/home/user/.ssh/
```

MAC ONLY – tighten permissions on your private key – command executed locally on your MAC

```
chmod 600 .ssh/private_key_name
```

Further key configuration:

Please refer to video lectures for configuration

Configure ssh key authentication:

```
cd /etc/ssh

sudo nano sshd_config
```

Restart the sshd service

```
sudo systemctl restart sshd
```

Login using SSH Keys

```
ssh -i .ssh/private_key_name user@ip
```

Example:

```
ssh -i identity_file user@server_ip_address

ssh -i .ssh/my_p_key andrew@123.456.789.101
```

Logout of server

```
exit
```

Config File - Commands Typed Locally

```
nano .ssh/config
```

Contents of config file

```
Host

HostName

User

IdentityFile

ServerAliveInterval 60

ServerAliveCountMax 120
```

Please refer to video lectures for creating your config file

To login, use:

```
ssh alias
```

Instead of:

```
ssh -i identity_file user@server_ip_address
```

FIREWALL

Install firewalld and then start the firewalld service and then enable it:

```
sudo yum install firewalld

sudo systemctl start firewalld

sudo systemctl enable firewalld
```

Firewalld commands:

```
sudo firewall-cmd --permanent --add-service=
```

Please refer to video lectures for adding services

List firewall rules:

```
sudo firewall-cmd --permanent --list-all
```

Commit and enable rules

```
sudo firewall-cmd --reload
```

FAIL2BAN

Install the EPEL repository

```
sudo yum install epel-release
```

Install fail2ban

```
sudo yum install fail2ban
```

Start and enable the fail2ban service

```
sudo systemctl start fail2ban

sudo systemctl enable fail2ban
```

Create a “jail.local” file:

```
cd /etc/fail2ban

sudo cp jail.conf jail.local
```

Please refer to the video lectures regarding configuring the first jail.

Once you have edited the jail.local file, save the changes to the jail.local file, then restart the fail2ban service

```
sudo systemctl restart fail2ban
```