Legend: Words inside quotations are the commands

Words that are italicized are words that need to be changed to make the command work and the italicized word describes what the word needs to be changed to.

When there are single quotation marks (‘ ‘) inside double quotations (“ “) the command requires double quotations where the single quotations are.

Phantom is based on CentOS so I am assuming that all CentOS commands will work on Phantom.

Reset Passwords:

1. Open a command prompt
2. Type “su” and your root password
3. To change the current user’s password type “passwd”,  hit enter
4. Then enter the new password

Confirm network information

1. Open command prompt
2. Type “ifconfig”

Enable Firewall as root

1. Open a command prompt
2. To enable the firewall type “systemctl enable firewalld”
3. To start the firewall type “systemctl start firewalld”
4. To see the status of the firewall type “systemctl status firewalld”
5. To list the firewall’s open ports type “firewall-cmd --list-all”
6. To open ports and services on the firewall
   1. To get the already configured services that can be enabled type “firewall-cmd –get -services” to get the already configured services that can be enabled
   2. To get the available zones type “firewall-cmd –get-zones” to get the available zones
   3. To add a service type “firewall-cmd –zone=*zone*–permanent –add-service=*service”*
   4. To add a port that is not already labeled as a service type “firewall-cmd –zone=*zone* –permanent –add-port *port #/protocol”*
   5. To reload the firewall type “firewall-cmd –reload”
   6. To confirm that the port was opened type “firewall-cmd –list-all
7. To close ports and services on the firewall
   1. To close a service type “firewall-cmd –zone=*zone* –permanent --remove-service *service*
   2. To close a port type “firewall-cmd –zone=*zone*–permanent –remove-port *port #/protocol*
   3. To reload the firewall type “firewall-cmd –reload”
   4. To confirm that the port was closed type “firewall-cmd –list-all
8. Ports that need to be open on Phantom TCP 22, TCP 80 and TCP 443

Firewall Instructions: <https://linuxconfig.org/redhat-8-open-and-close-ports>

Repository:

1. Open command prompt
2. To list the repositories type “yum repolist”
3. To view a detailed list of the repositories type “yum -v repolist”
4. To view a list of all the repositories available type “yum repolist all”.  This view will also tell you which repositories are disabled.
5. To view a list of just the enabled repositories type “yum repolist enabled”
6. To view a list of just the disabled repositories type “yum repolist enabled”
7. To see the installed packages versions and the repository type “yum list installed”

Change sshd\_config file:

1. Open command line
   1. To open the file type “cat /etc/ssh/ssh\_config”
   2. To edit the file type “nano /etc/ssh/ssh\_config”
2. To change the location of the ssh\_config file
   1. type “su” then the root password
   2. Change the directory to /etc/ssh/ by typing “cd /etc/ssh/”
   3. List the files in the directory by typing “ls”.  This just makes sure that we are in the right location and that the ssh\_config file is there.
   4. Then type “mv ssh\_config ~/*location*”.  I moved mine to the documents folder, so my command looked like mv hosts ~/Documents

Identify and change hosts file

1. Open a command prompt
2. The file’s location is /etc/hosts
3. To edit the file type “nano /etc/hosts”
4. To change the location of the hosts file
   1. type “su” then the root password
   2. Change the directory to /etc/ by typing “cd /etc/”
   3. List the files in the directory by typing “ls”.  This just makes sure that we are in the right location and that the hosts file is there.
   4. Then type “mv hosts ~/*location*”.  I moved mine to the documents folder, so my command looked like mv hosts ~/Documents

To change the Phantom dashboard admin password

1. This will need to be done from the Debian machine
2. Click on admin in the top right
3. Click on the change password in the top middle of the screen
4. Then change the password to whatever you want and hit change password

How to update the OS

1. Open a command prompt
2. In the command line type “yum check-update”
3. The mirrors that came up for updates were:
   1. base: mirror.us-midwest-1.nexcess.net
   2. extras: mirrors.tripadvisor.com
   3. updates: us.mirror.nsec.pt

List users on the computer

1. Open a command prompt
2. Type cat /etc/passwd
3. To show just the username of the user’s type “awk -F':' '{ print $1}' /etc/passwd”

How to install an antivirus

1. Open a command prompt
2. Type “yum -y update”
3. Type “yum -y install epel-release
4. Type “yum -y update”
5. Type “clean all”
6. Type “yum -y install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd
7. Type “setenforce 0”
8. Type “setsebool -P antivirus\_can\_scan\_system 1
9. Type “setsebool -P clamd\_use\_jit 1”
10. Type “getsebool -a | grep antivirus”
11. Type “yum -y install nano”
12. Type “nano /etc/clamd.d/scan.conf”
    1. When the file opens get rid of the word example that is in the top of the document
    2. Save the file
13. Type “cat /etc/passwd | grep clam”
14. Type “nano /etc/clamd.d/scan.conf”
15. Scroll down in the file and find these lines
    1. # The daemon can work in local mode, network mode or both.
    2. # Due to security reasons we recommend the local mode.
    3. # Path to a local socket file the daemon will listen on.
    4. # Default: disabled (must be specified by a user)
    5. #LocalSocket /var/run/clamd.scan/clamd.sock
    6. Get rid of the hashtag next to the localsocket
16. Save the file
17. Type “cp /etc/freshclam.conf /etc/freshclam.conf.bakup”
18. Type “sed -i -e "s/^Example/#Example/" /etc/freshclam.conf”
19. Type “freshclam”
20. Type “systemctl start clamd@scan”
21. Type “systemctl enable clamd@scan”
22. Type “systemctl status clamd@scan”
    1. This will output the status of clamd@scan
23. Type “clamscan –infected –remove –recursive –exclude-dir=’^/sys’ /”
    1. This will scan your entire machine for viruses and will take a long time

How to install NTP

1. Open a command prompt
2. Type “yum install ntp”
3. Type “/etc/ntp.conf”
   1. Edit the file so that the server is 172.20.242.200.  This will point the ntp on the client to the server ntp.
4. Type “systemctl start ntpd.service”