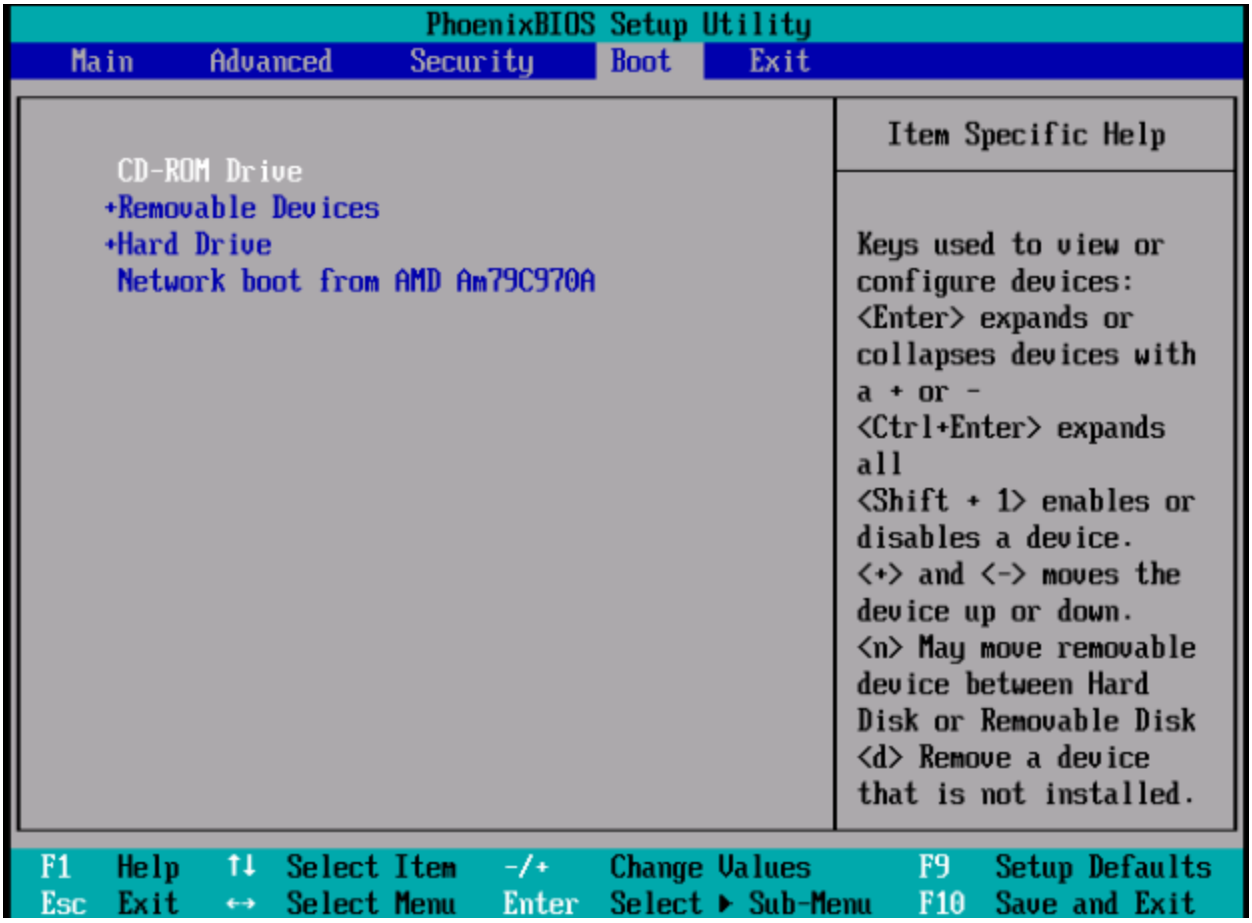
Interested in learning more about security?

SANS Institute

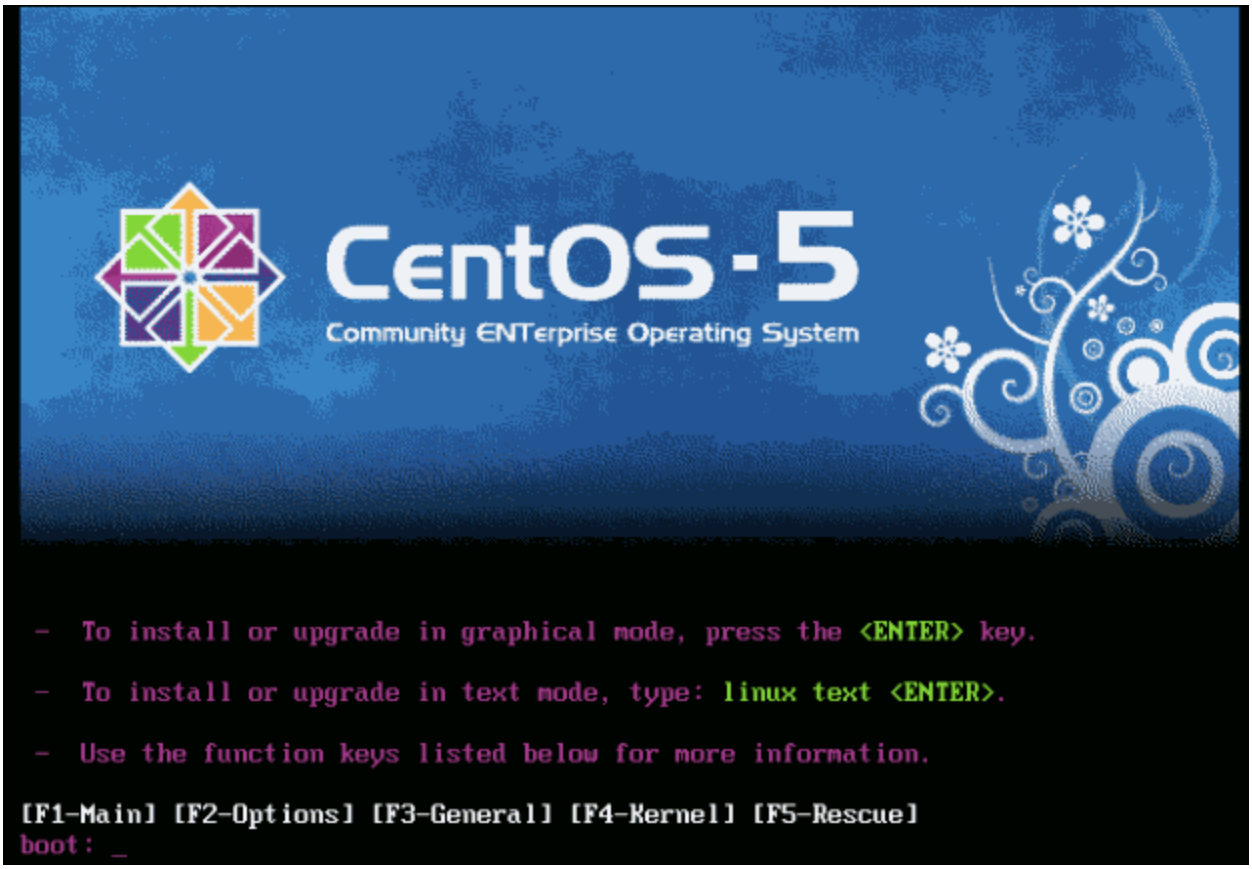
Security Consensus Operational Readiness Evaluation

SCORE Security Checklist

Install



Make sure your system is set to boot from CD-ROM/DVD drive first
There are also network-based and USB-based installation options. Any will work, though these two take additional work. Once you boot the install media, continue.



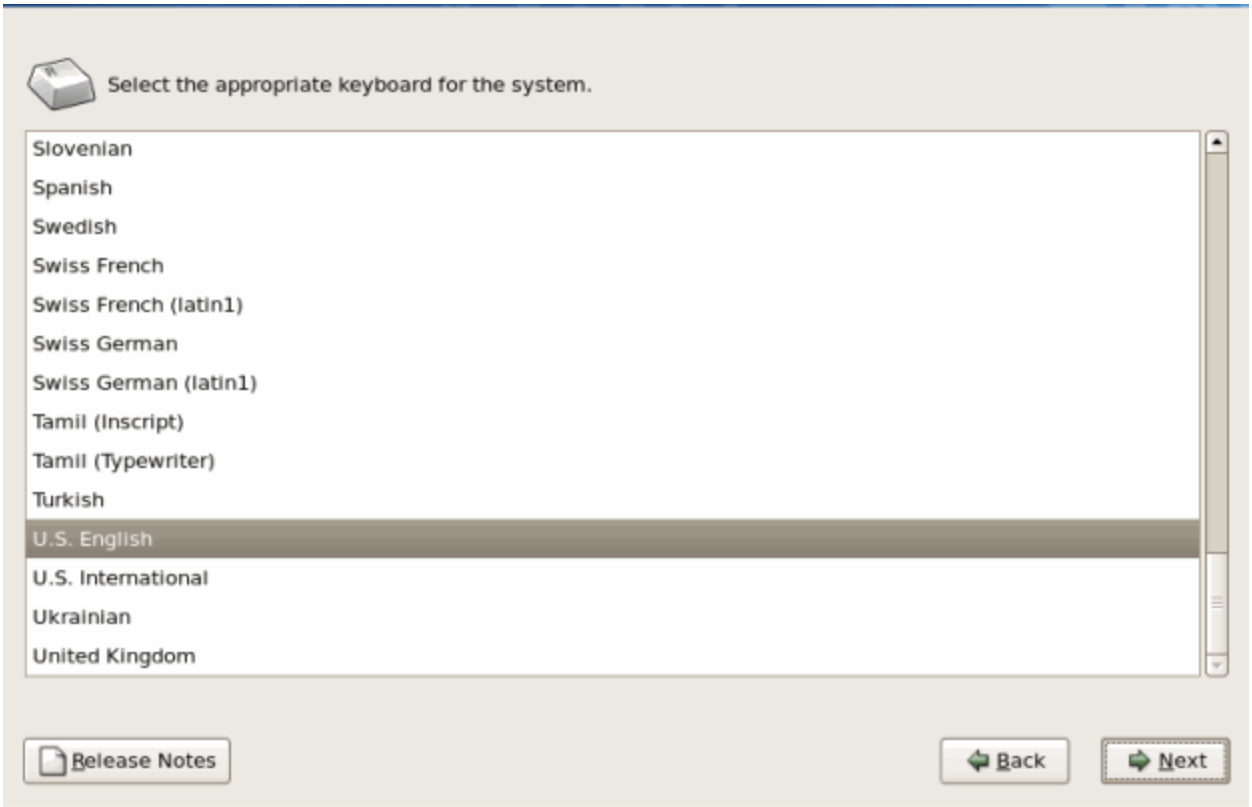
At the boot screen just hit enter to install in graphical mode (default)

You can run this check if you would like. This will check the MD5 Checksum of all of the disks. This takes a very, very, very long time. I normally choose Skip on this step. If there is a media

error, you will know sooner and be able to produce new media in the time the check would take to tell you it is bad.

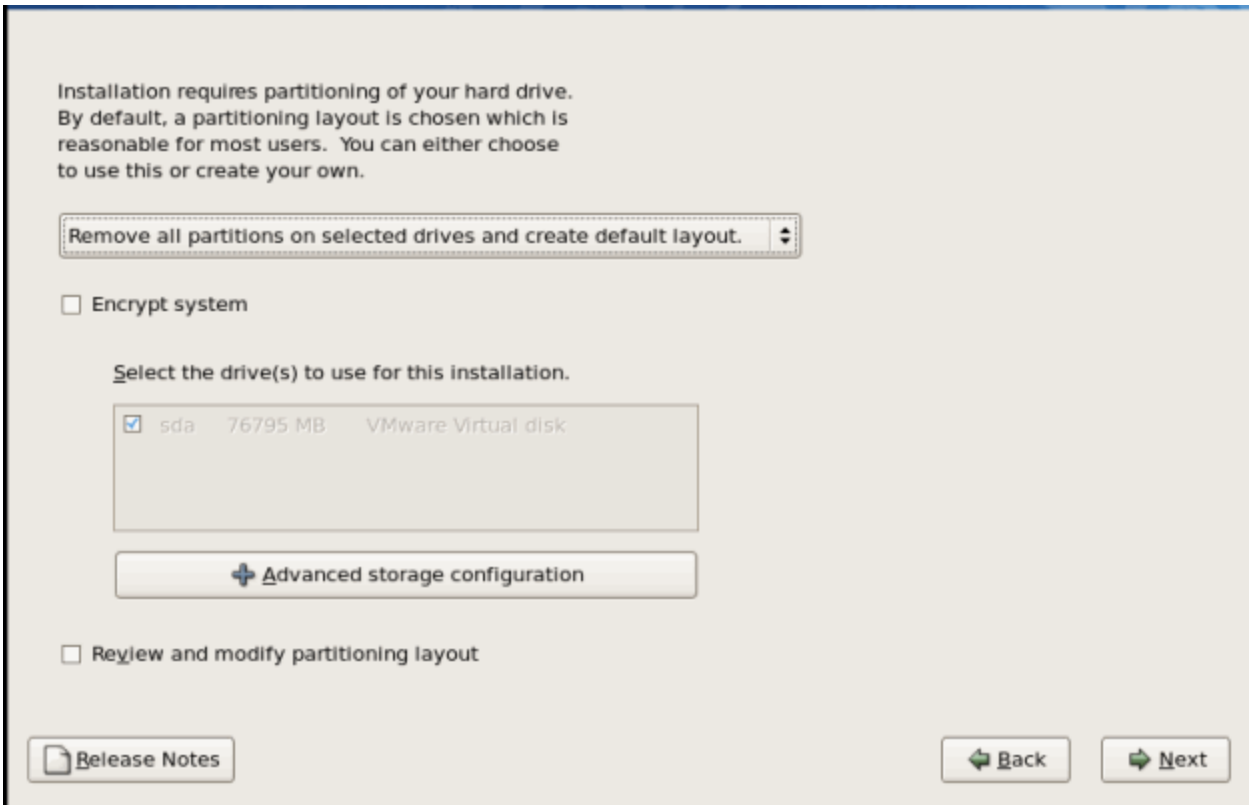
Choose next from the Welcome Screen

You will choose the language next. Here we will keep the default choice of English (English) and click next.



You can choose your keyboard layout next. Again, here we will be accepting the default of U.S. English.

You may see this error if you have a new drive with no partitions. We will click yes on this one for our example. You may want to choose no and back up your data first if this is not OK.

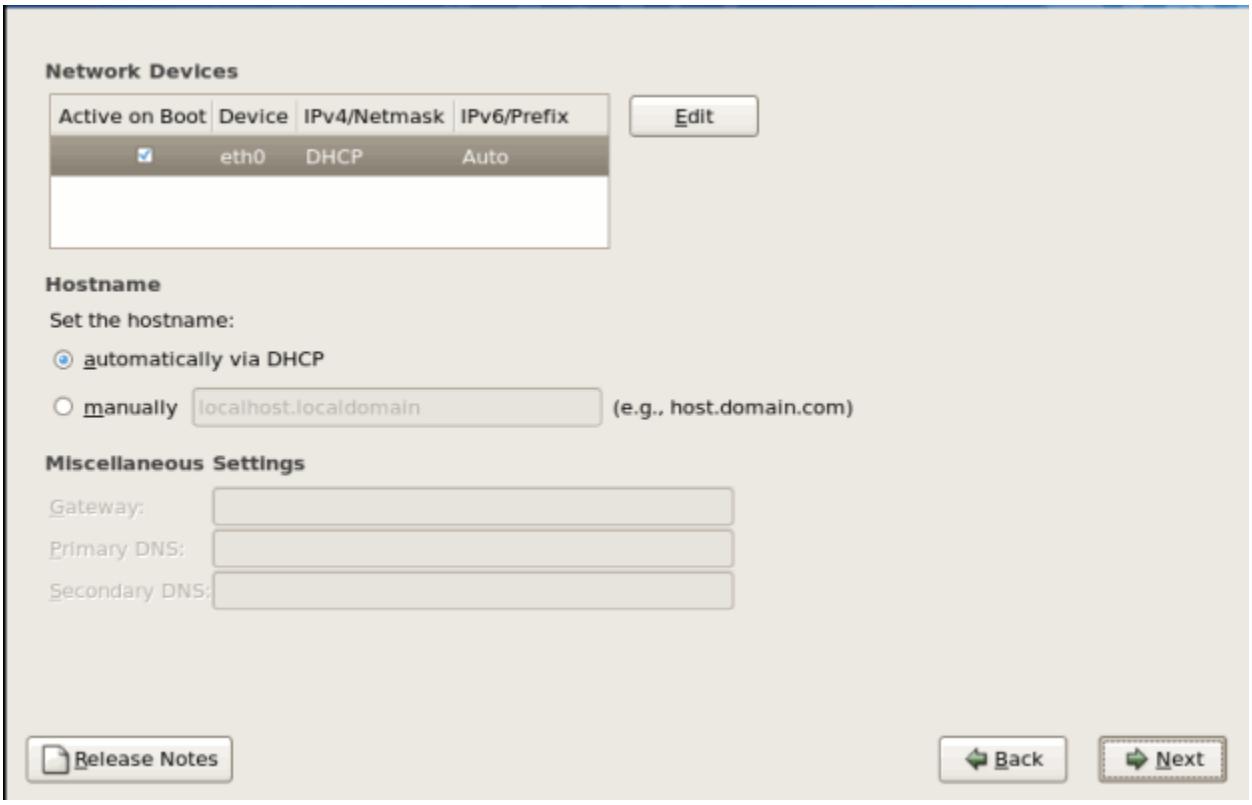


Here you can choose how to partition your hard drive. Your choices are to remove all partitions on the selected drives and create the default layout, remove Linux partitions on the selected drives and create default layout, use free space on selected drives and create default layout and create custom layout. You can also choose to encrypt the system. Here we will choose remove all partitions on the selected drives and create the default layout.

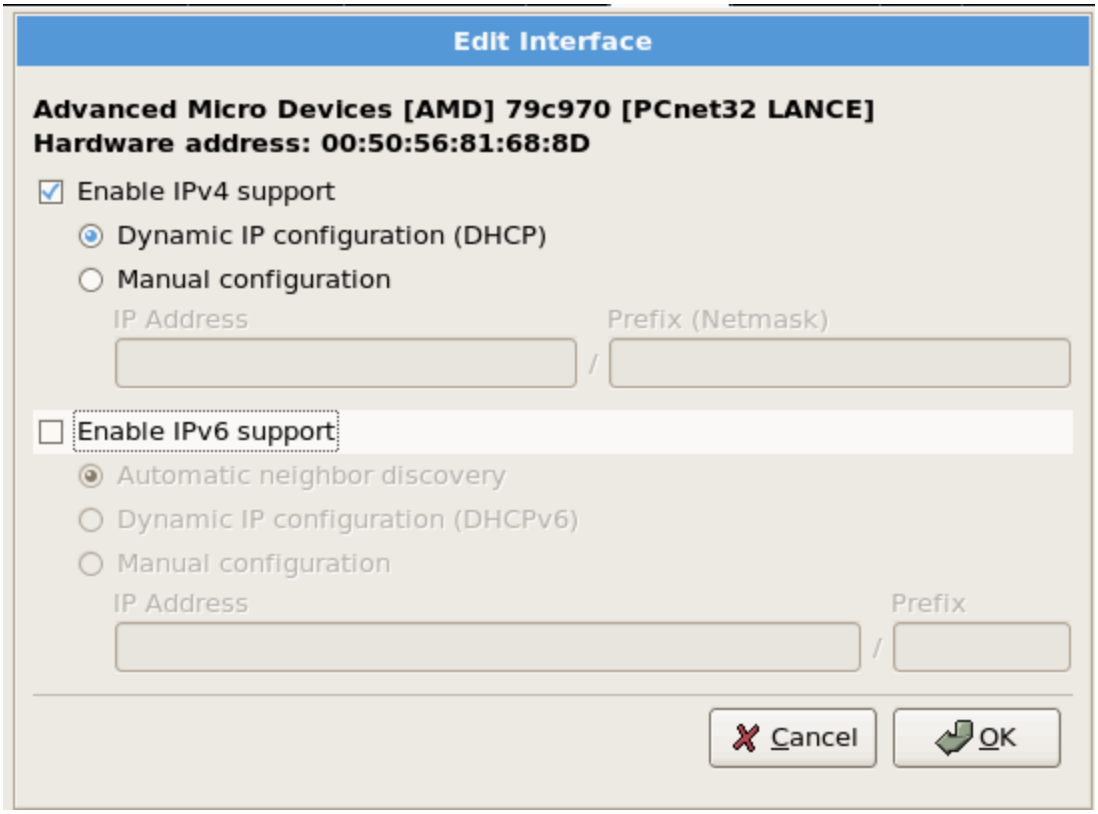
Two notes on encryption:

1. If you choose to encrypt the partitions, a password will need to be entered every time the system boots up. This may be fine in some places, but if you have a system in an unmanned datacenter, it could be difficult to deal with. You can make a choice to encrypt a volume after installation if you require encryption on some of the data.
2. On a server, disk-level encryption doesn't gain you much. If the machine is always on, the kernel always has the disks decrypted. Disk-level encryption makes more sense on a laptop.

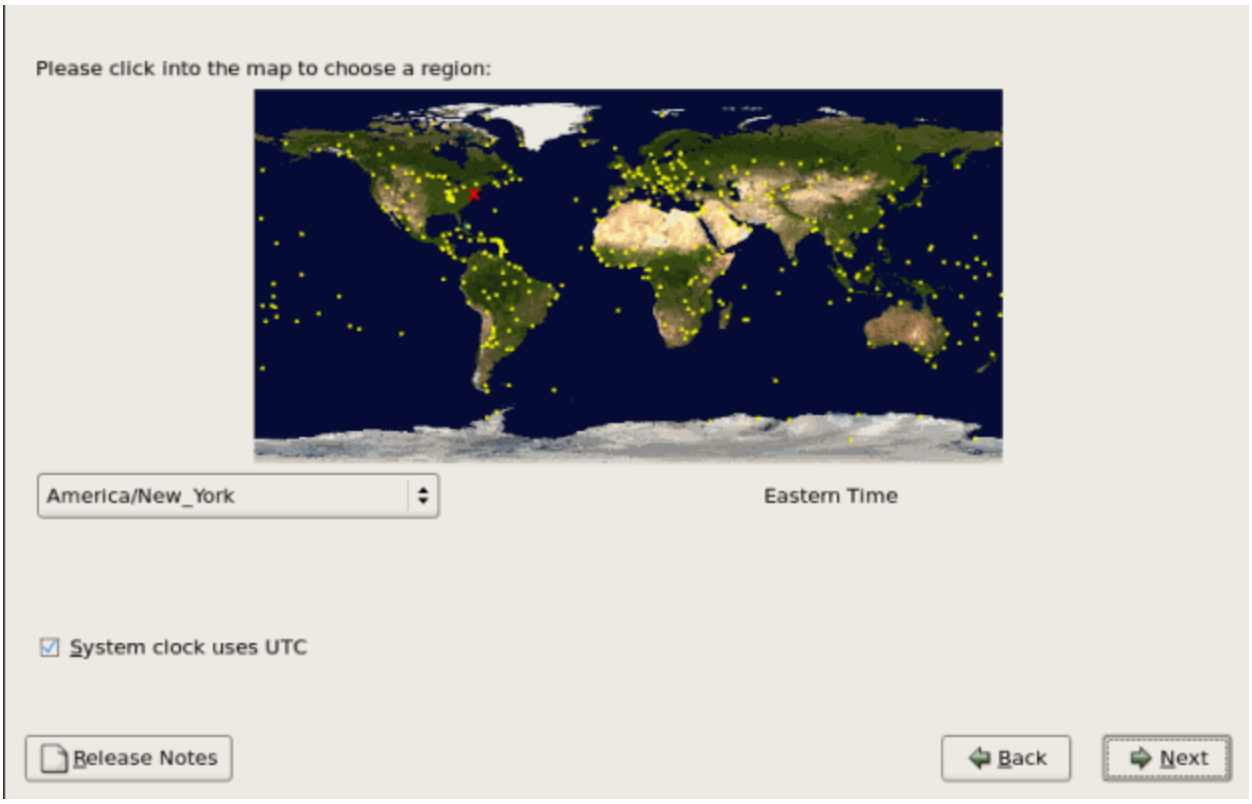
Once you are sure you want to proceed, choose yes.



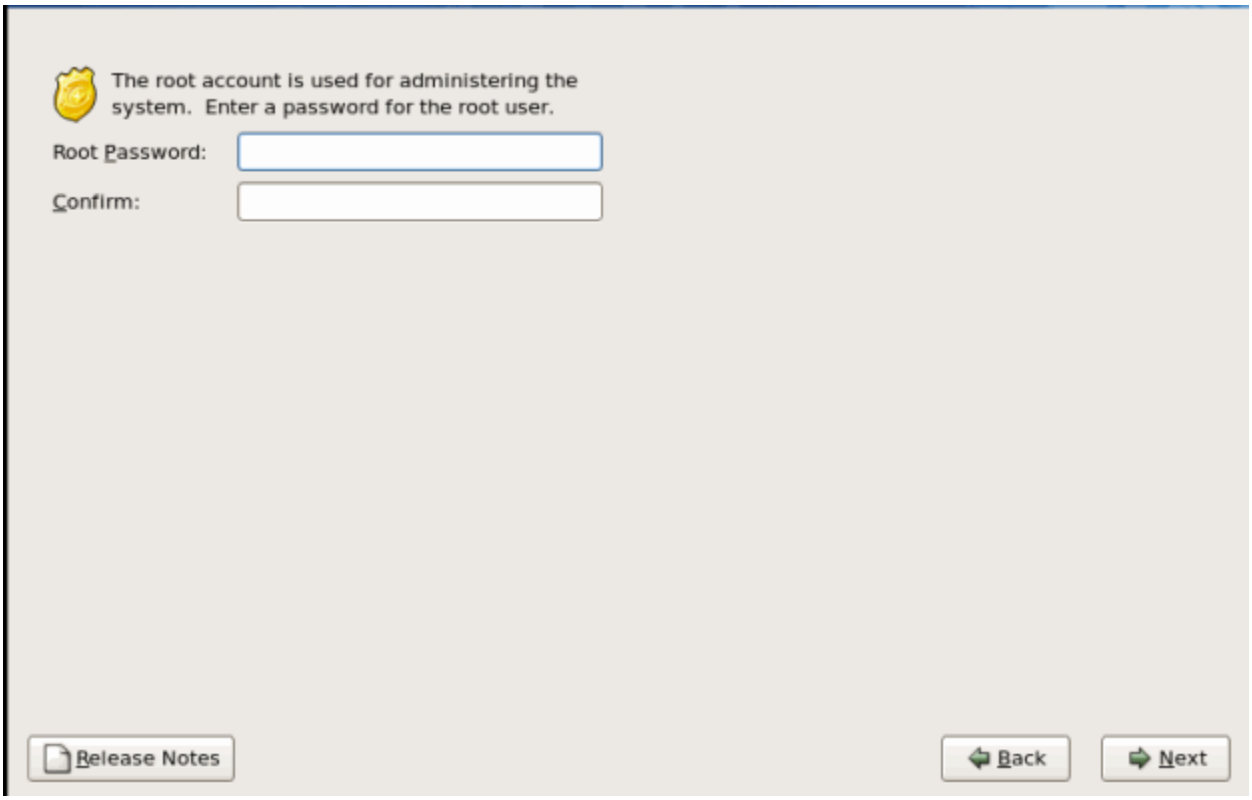
Next you will have the chance to set your network settings. If you want to change the device from DHCP to a static IP address, for example, click the Edit button. You can also specify your domain name here by choosing to set it manually. Finally you can modify your default gateway, primary DNS and secondary DNS. These final options are only available if you choose to create a static IP address. We are leaving this blank for this example. We will set the IP after the installation.



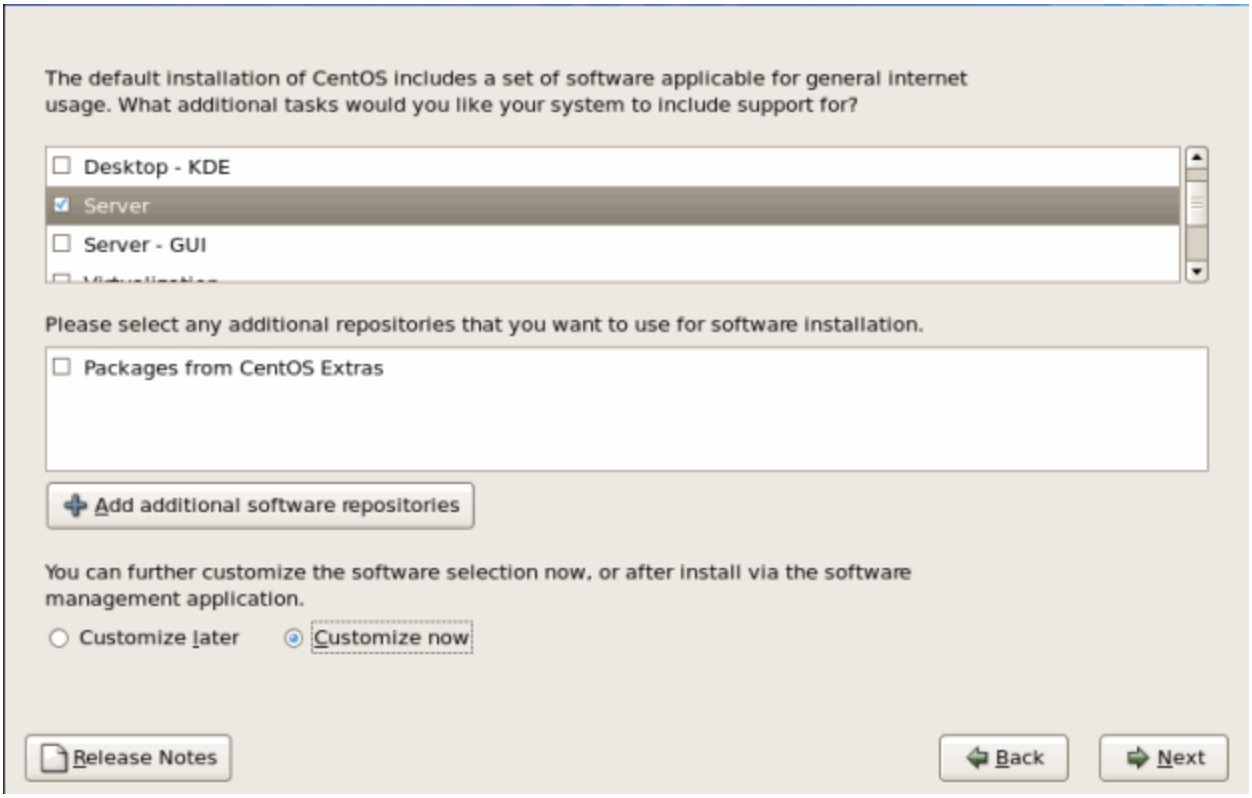
The only other security related setting you may want to change is in the Edit menu. Disable the IPv6 support unless you will be using it. IPv6 is still relatively new and there have been security issues with how it is implemented in the kernel. Do not leave it on “just in case”. Remove it now, you can add it back when you want later. A service that is not installed and running cannot be compromised.



Next you should choose the time zone you are in. In our example, we will keep the default America/New_York Eastern Time

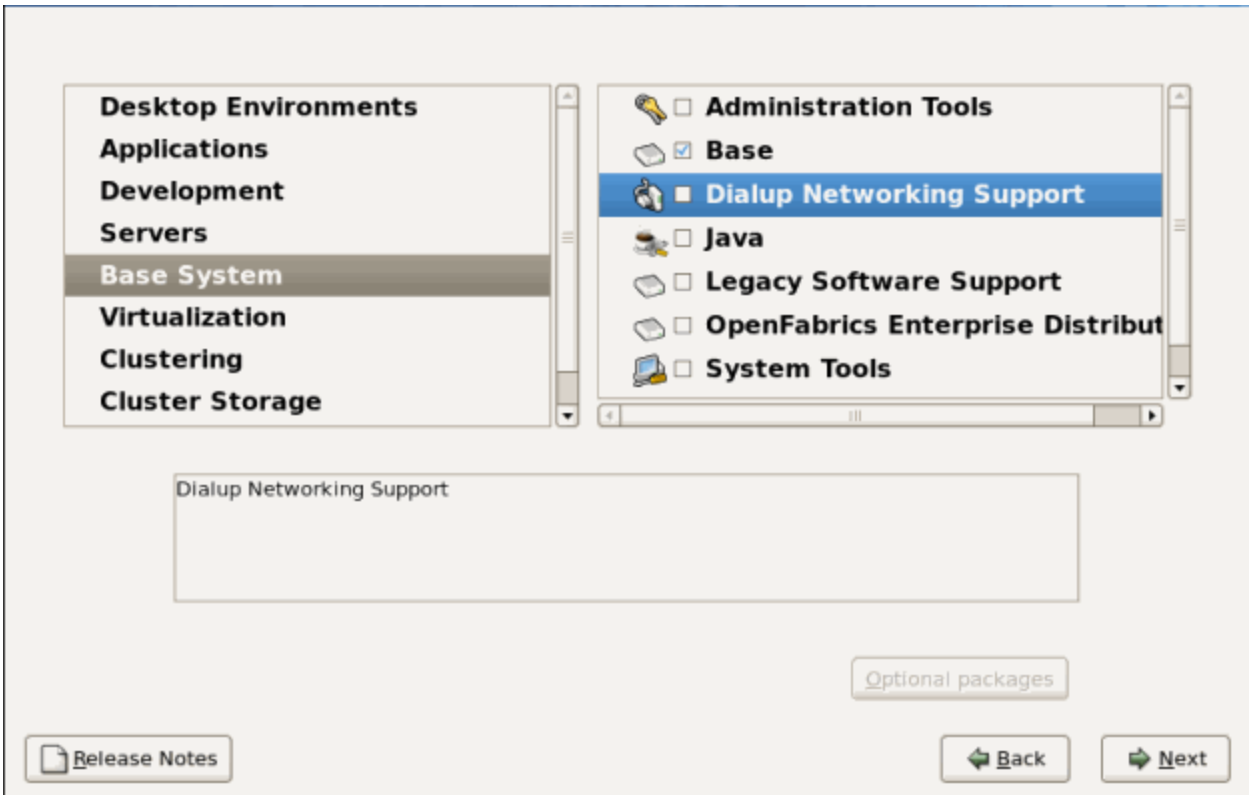


Next you will need to set you root password. This should be a password that is very difficult to guess and a sufficient length. We will use the a minimum of 15 characters in our example. You can also take some further precautions after the installation such as restricting root from logging in via SSH and using PAM modules to allow RSA token use.

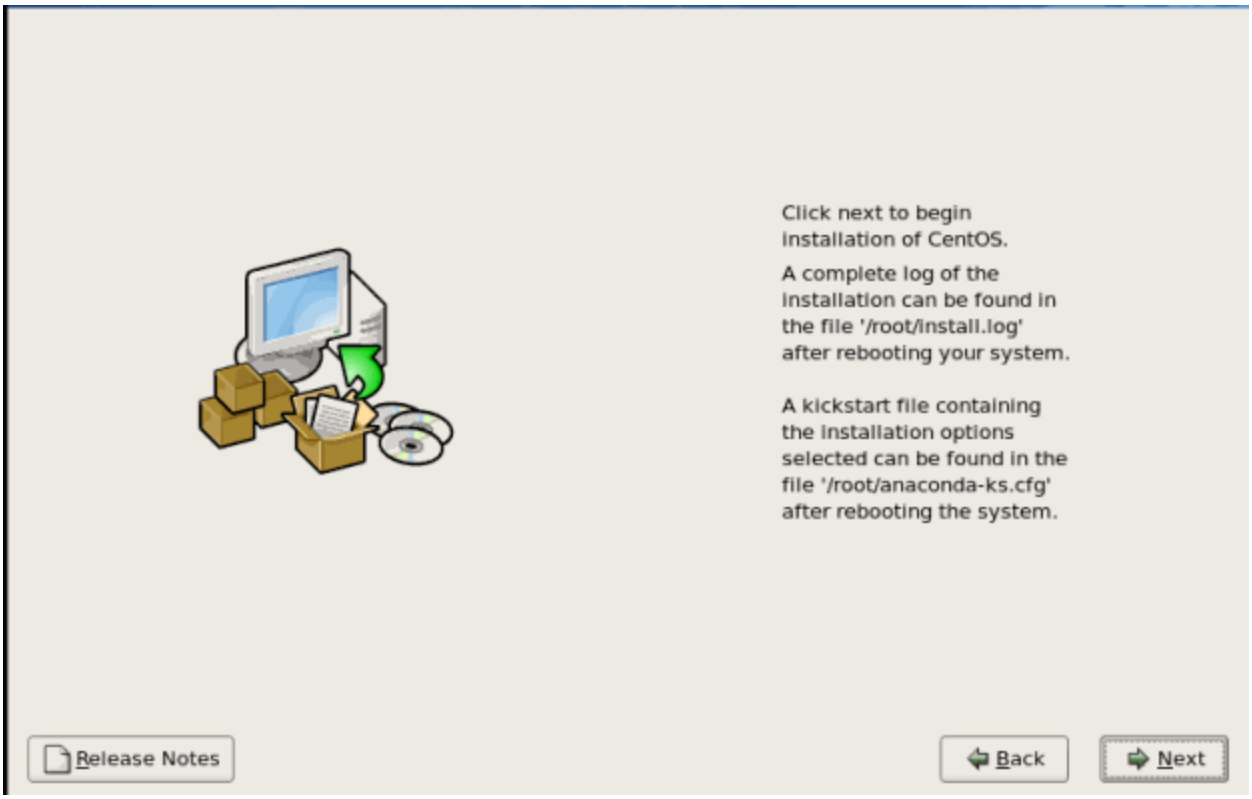


Next, you can choose the packages you would like installed. Here we are building a server so we are going to choose the Server option. Do not put GUIs on the server builds unless it is specifically required. This will lower the overall footprint and security posture of the system. Again, if it's not installed, you don't have to worry about security holes in it. I will also choose the Customize now option so we can pick and choose which Server options we want.

This system will be a web server. With that in mind, we have left the defaults up to the Servers section. The previous defaults include nothing selected in Desktop Environments. In applications, the only things selected by default are Editors and Text based Internet. Nothing is selected in the Development section. The default in the Servers section is everything selected. Remove all options that you will not be using. In this example, we only leave Web Server selected.

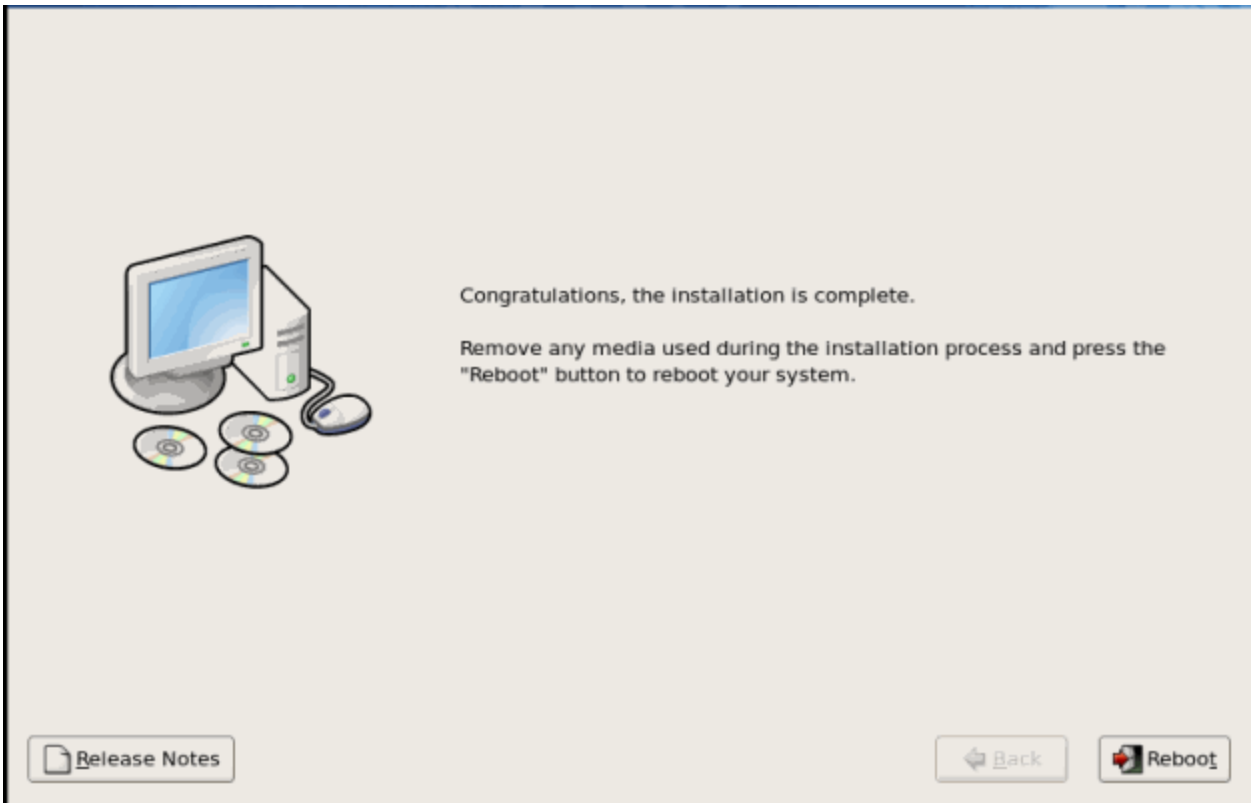


Under the Base System, we will remove the default selection of Dialup Networking Support and leave the rest of the defaults. We will leave Virtualization, Clustering and Cluster Storage in the default state of nothing selected.

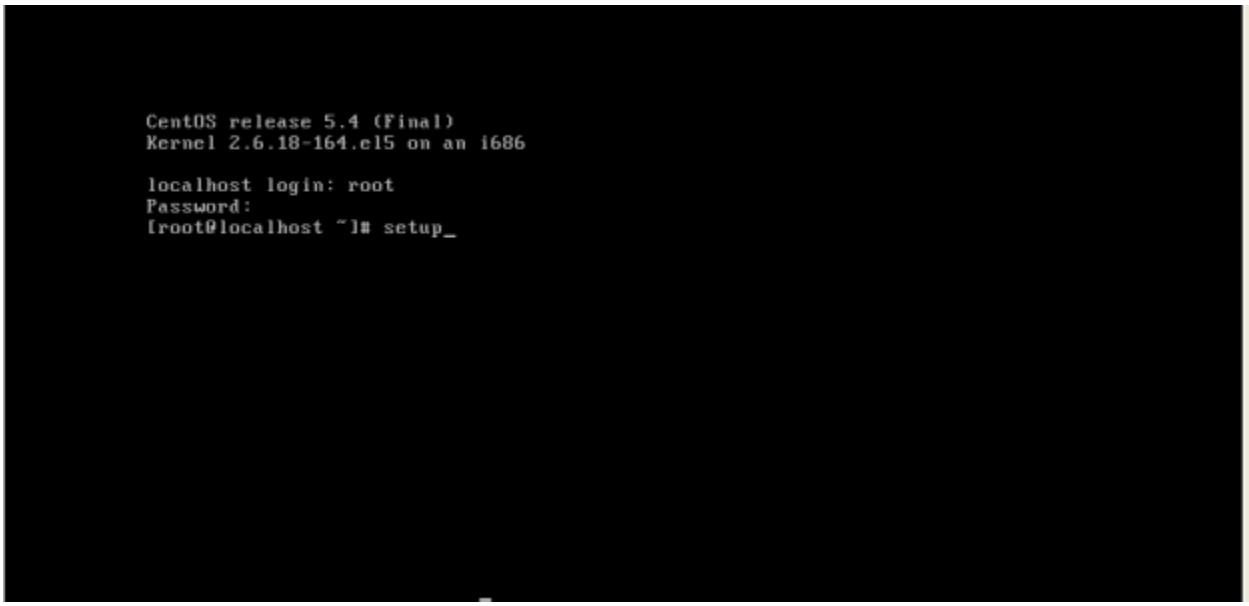


Here we just choose next to begin the installation.

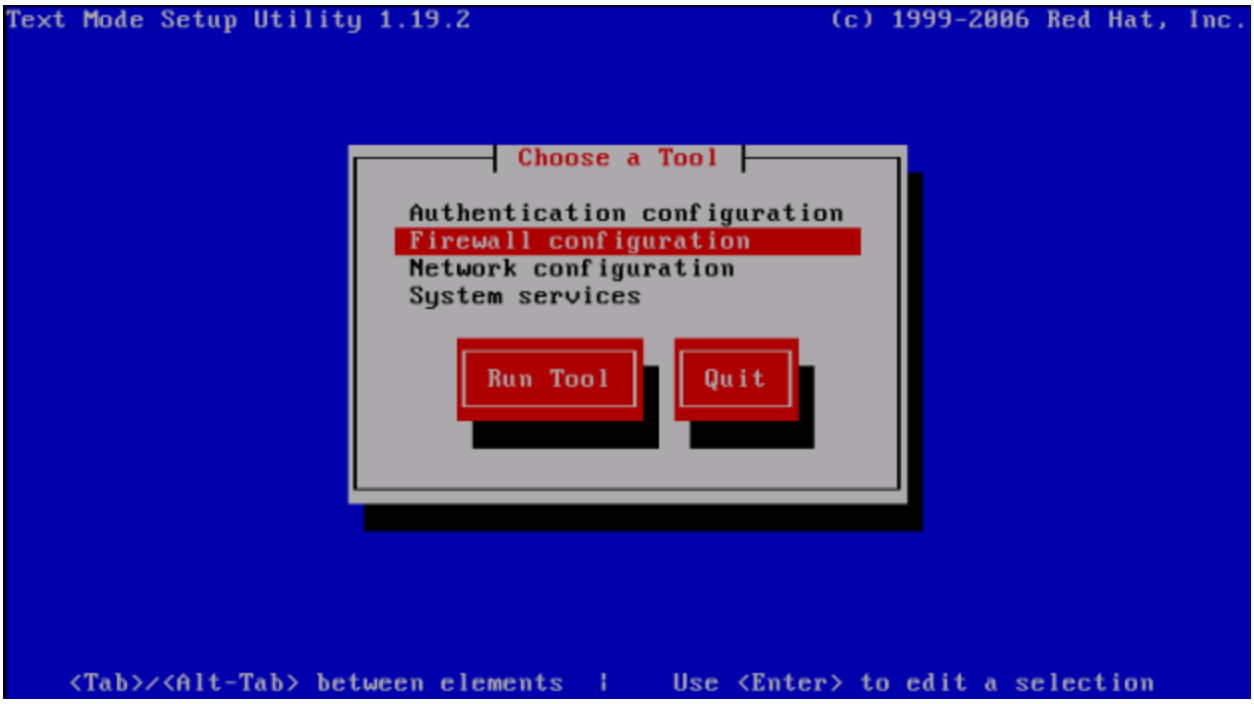
The installation will show you which disks you will need to install the software you selected. Ensure you have all of the necessary disks and click continues. If you do not want to continue you can choose Reboot or if you have selected something by mistake or are unsure, you can choose the Back option.



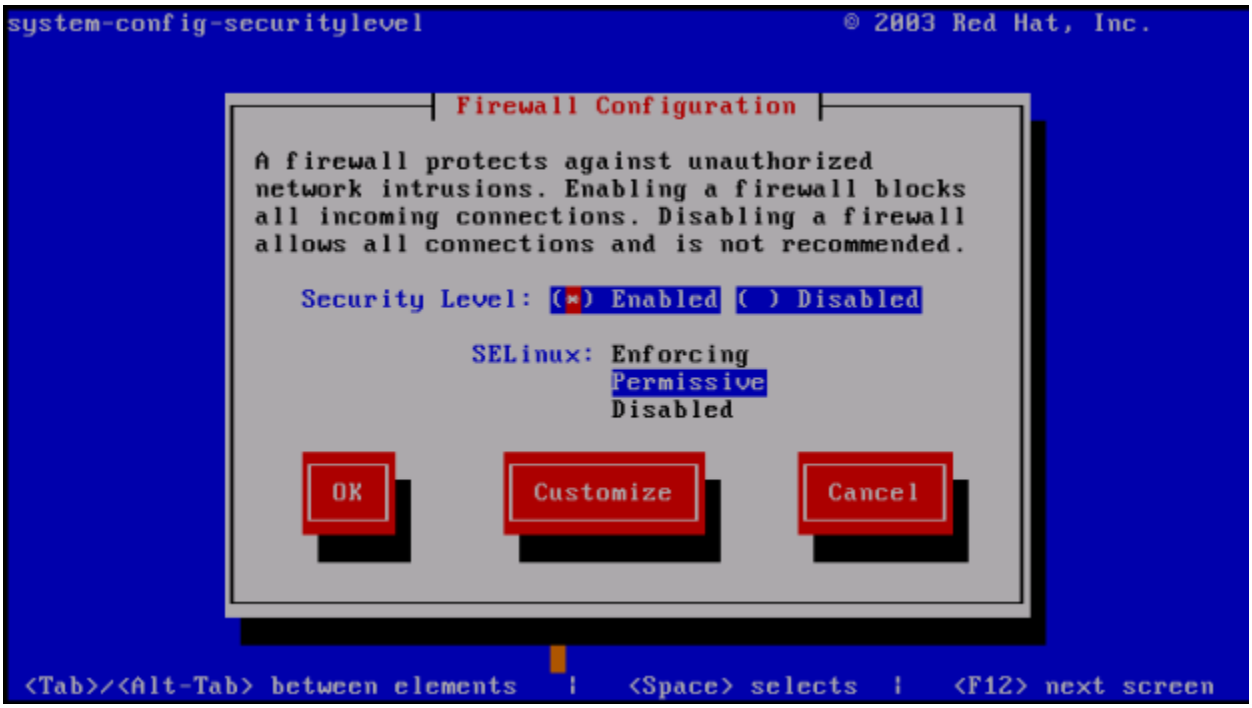
After the installation, choose Reboot to complete the process.



After the reboot, log in as root. Type the command “setup” without quotes. This is an ncurses menu driven application that allows you to configure a CentOS or Redhat system from a command line with a GUI feel.



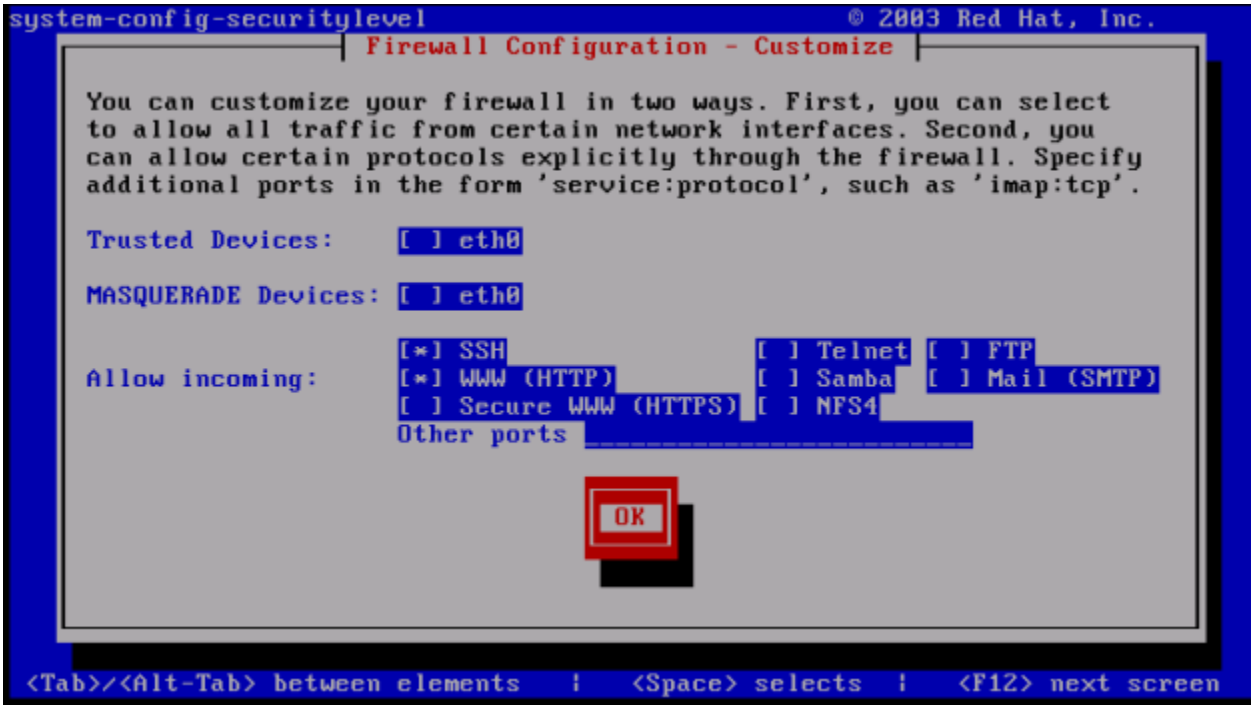
The first thing we will do is ensure that the firewall is on and only allowing ports we expect through. Choose the firewall option, hit tab to move the focus to the Run Tool button and click enter.



**

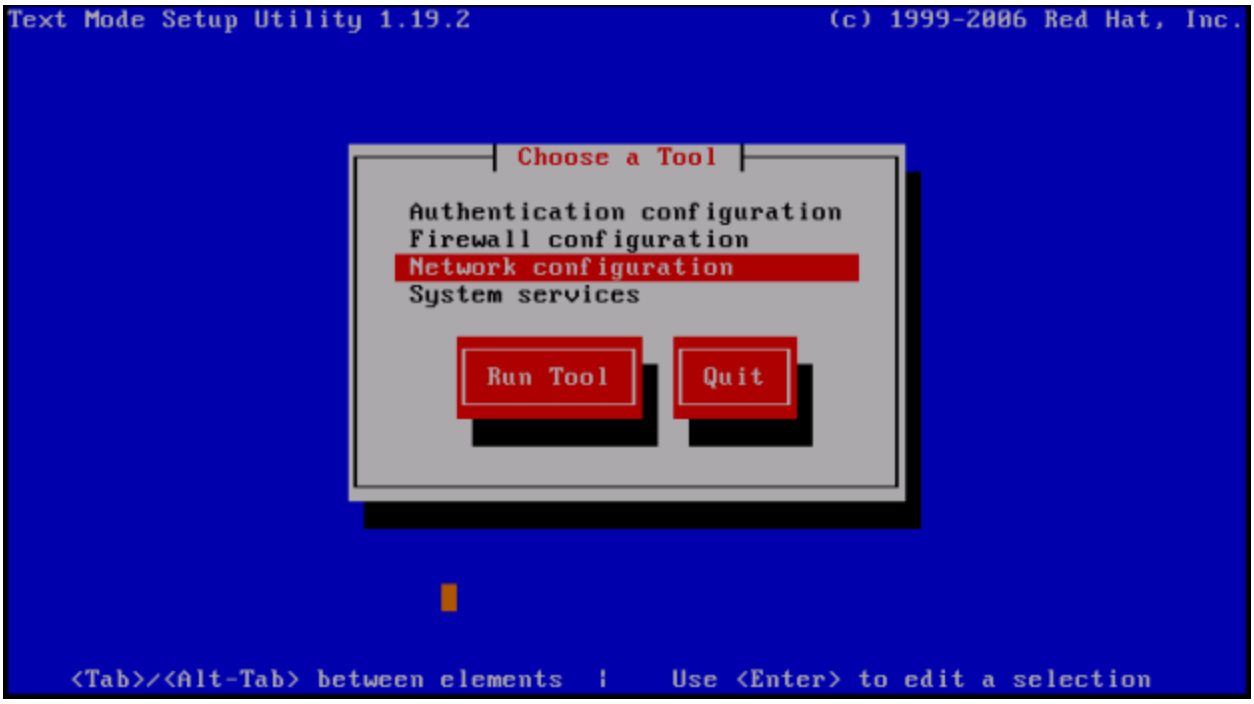
For our options in this example we will be making sure the security level is enabled and we will set SELinux to Permissive. We prefer Bastille to SELinux due to easier configuration. We do leave it as Permissive to get the logging it provides.

NOTE TO OTHERS: I disagree with this piece of advice. On a packaged system, admins are better served learning to use the "standard" tools. Thus, on RHEL, they should use SELinux and on SLES/Ubuntu, they should use AppArmor. Bastille may well be a good option, but it should be offered as an addition/option to this guide, not as the default. -Josh More

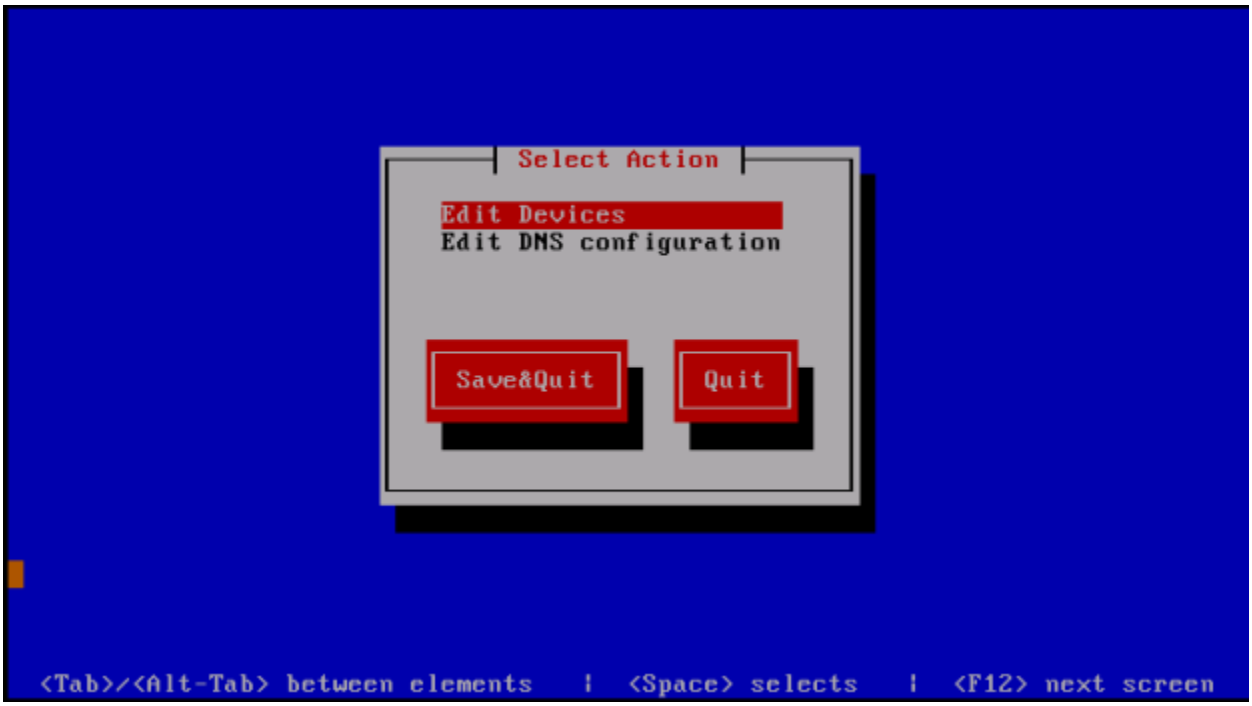


Click the Customize button on the previous screen and you will see this screen. For our example, we need to manage the system so we allow SSH as an incoming connection. We also want this to be a web server in this example so we will also allow WWW (HTTP) as incoming. Make the allowances for the necessity of the system. The main thing is to only allow what is absolutely necessary.

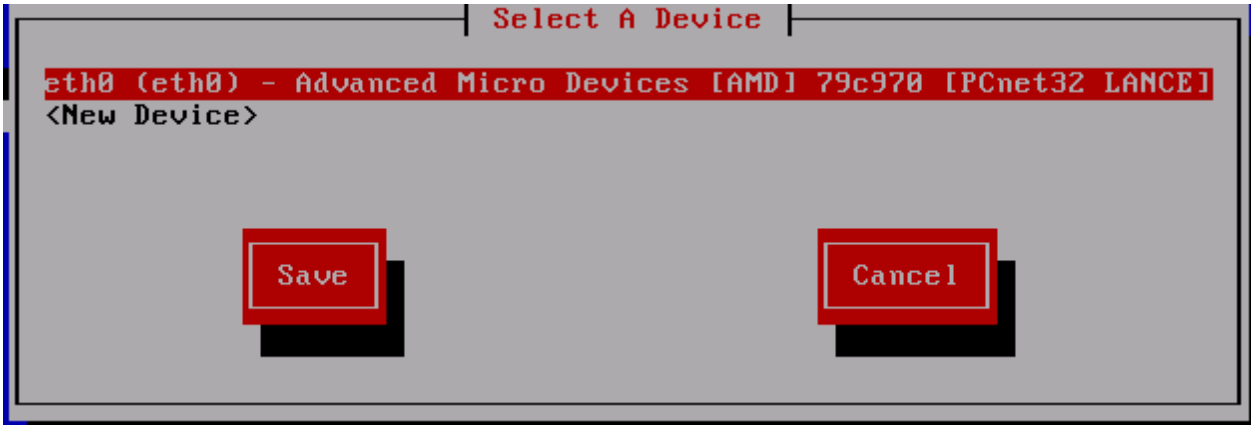
At a later stage, we will control access via SSH to only allow connections from secured networks. In order for HTTP to be functional, it must by default listen to the entire Internet. SSH does not need this. You must access it for admin reasons, but this is from a much smaller range of hosts. The configuration should be limited to known-good access points.



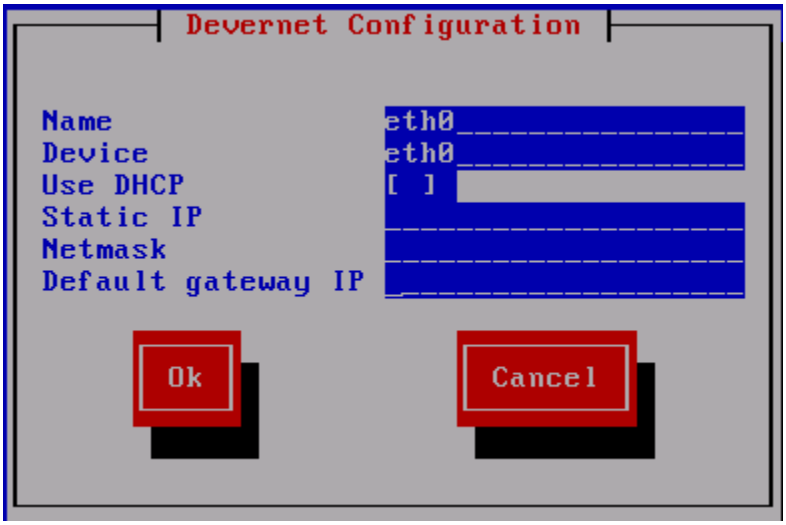
Next we will choose Network Configuration. We are doing this now in this example because we did not set an IP address in the setup. If you did set the IP address in the setup, you can skip this step.



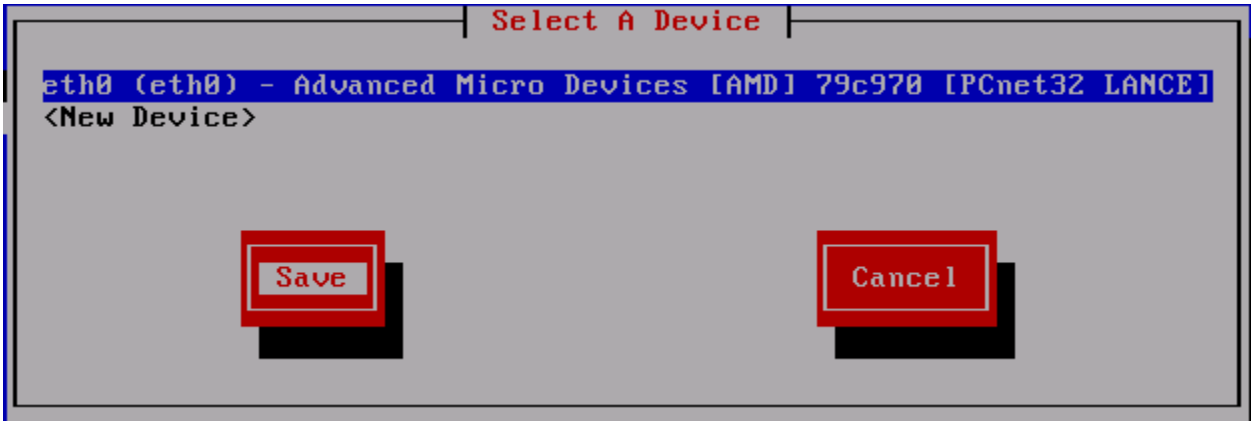
Highlight the Network configuration option. Hit the tab key to move the focus to the Run Tool button and click enter. Choose the Edit Devices option.



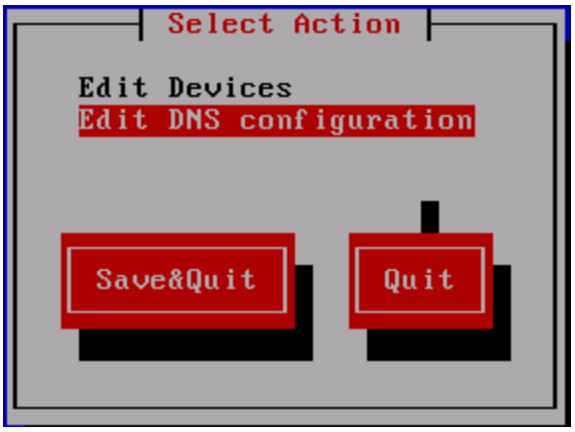
Hit enter on the Edit Devices menu and you should see a similar screen. You may see more interfaces if your system has more installed.



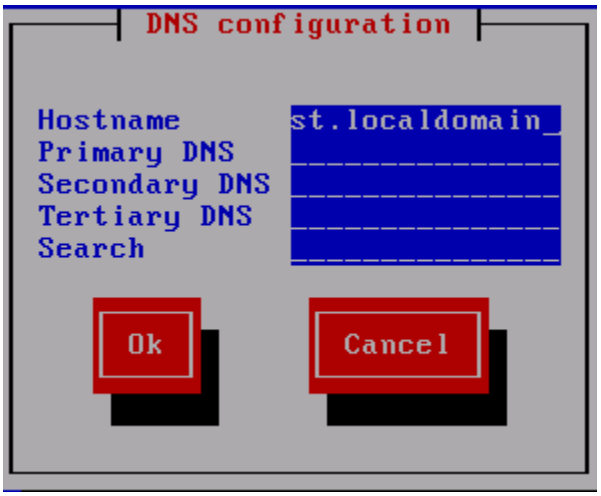
Hit Enter on the device you want to configure. Remove the * from Use DHCP . Enter the IP address, subnet mask and default gateway of your system. After you are done, hit the tab key to put the focus on the OK button and hit enter.



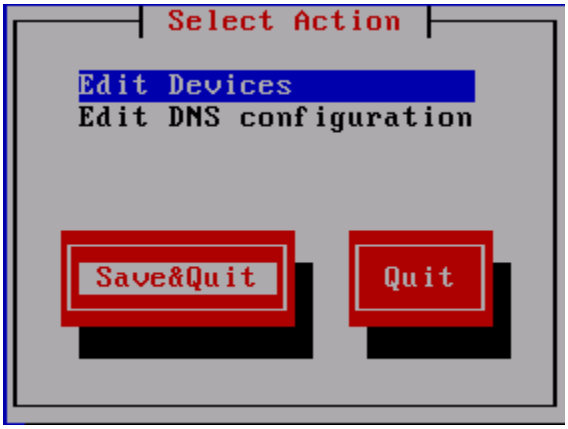
Hit the tab key to put the focus on the Save button and hit Enter.



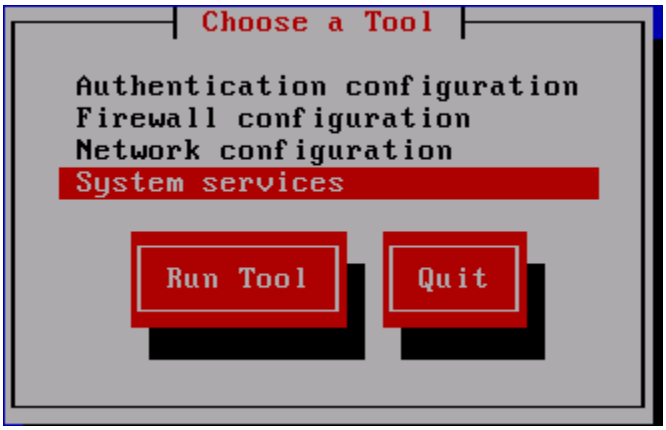
Put the focus on the Edit DNS configuration option and hit the Enter key.



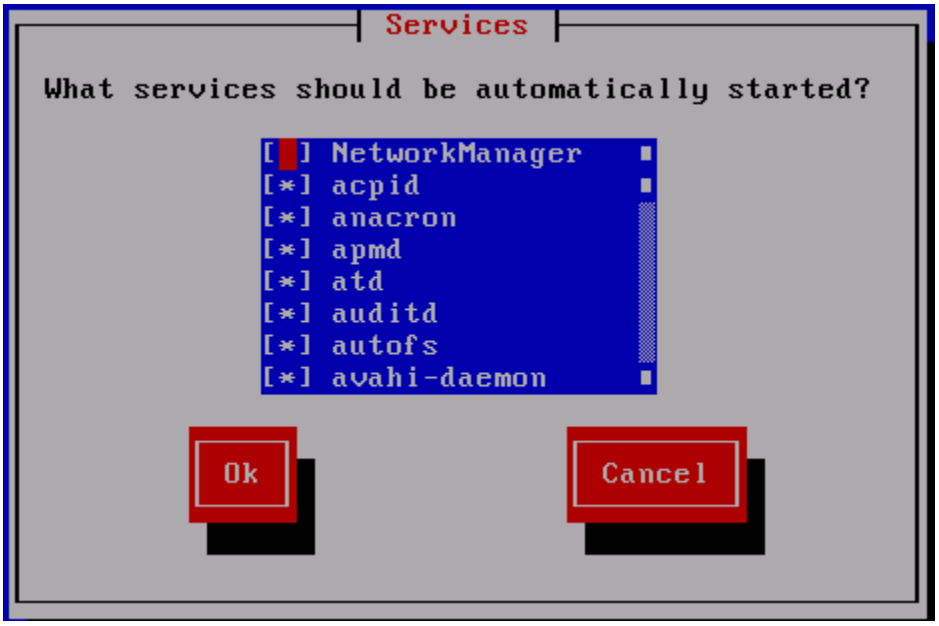
Enter the FQDN hostname of the system here along with the Primary DNS, Secondary DNS, Tertiary DNS if you have one and any domains you would like to add in the search order. This option is useful if you have multiple domains or subdomains in your network. After entering the information hit the tab key to put the focus on the OK button and hit the Enter key.



After entering all of this information, hit the tab key to put the focus on the Save&Quit option and hit the Enter Key.

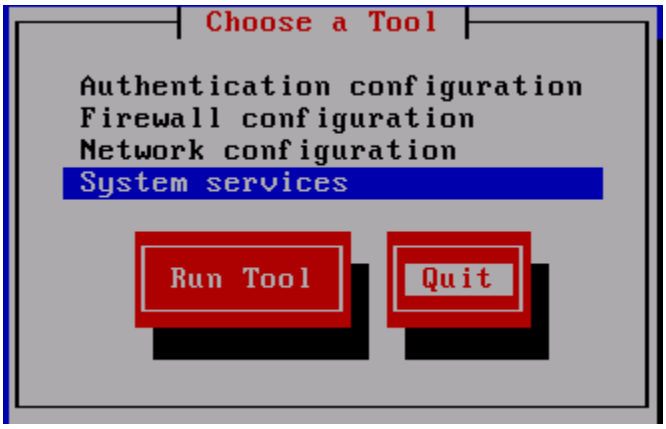


Put the focus on the System Services option, hit the tab key to move the focus to the Run Tool button and click Enter.



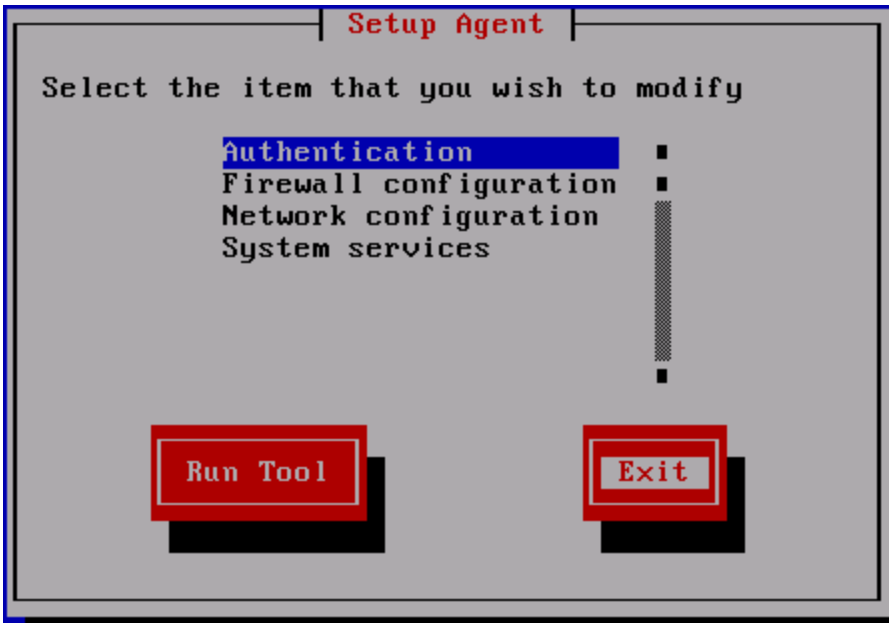
What services you choose to turn off or on here depends on the type of system that this is. The main idea is to turn off everything you can that you don't need. You can always turn on the things you need later. This setting is to say what services will be automatically started when the system boots. Below is a list of things I generally turn off on all systems. The other thing I will be turning on in this system is the Apache web server (called HTTPD in this version).
Services to generally turn off unless speficially needed:
APMD
Bluetooth
CUPS
IP6TABLES (unless you are using IPv6)
ISDN
NETFS
NFSLOCK

PCMCIA
PORTMAP
XINETD (unless you're using an xinetd-wrapped service. More on this later.)



Hit the tab key until the focus is on the Quit button and hit Enter.

At this time you should reboot the system to ensure the changes are applied.



You may be faced with this screen after rebooting. Just hit tab until the focus is on Exit and hit the Enter key.

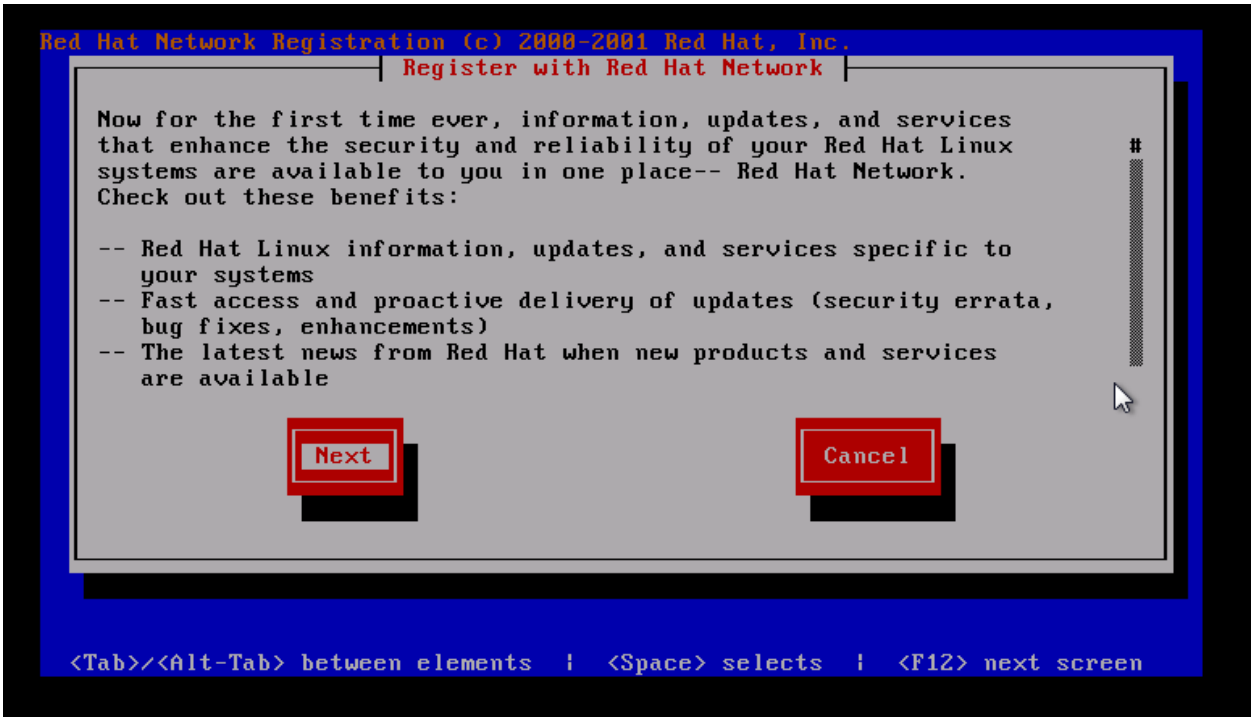
Patch

Log in as root on the console.

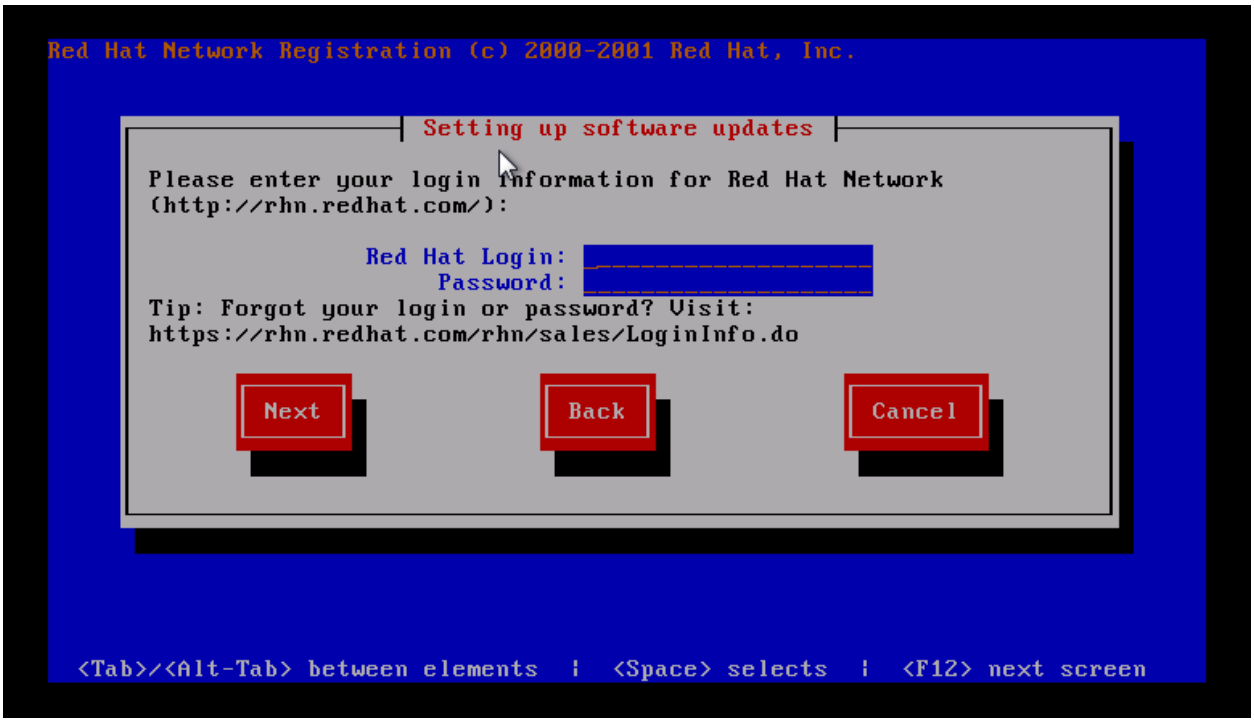
Red Hat Enterprise Linux v.5 uses yum (like CentOS and Fedora). Red Hat Enterprise Linux up to and including v.4 uses up2date. Regardless of which version of Red Hat is installed, the system profile will need to be registered with the Red Hat Network before any OS updates or patches can be downloaded and installed. To register with Red Hat Network, a user account must have already been created. If you do not already have a user account, go to https://rhn.redhat.com/rhn/sales/LoginInfo.do. Setting up a Red Hat Network user account is outside the scope of this document. To register the system profile, use the rhn_register command with the no-graphics option. The screenshots demonstrating the registration are from a RHEL v.4 system. RHEL v.5 systems will look similar.

```
[root@seedbug ~]# rhn_register --nox_
```

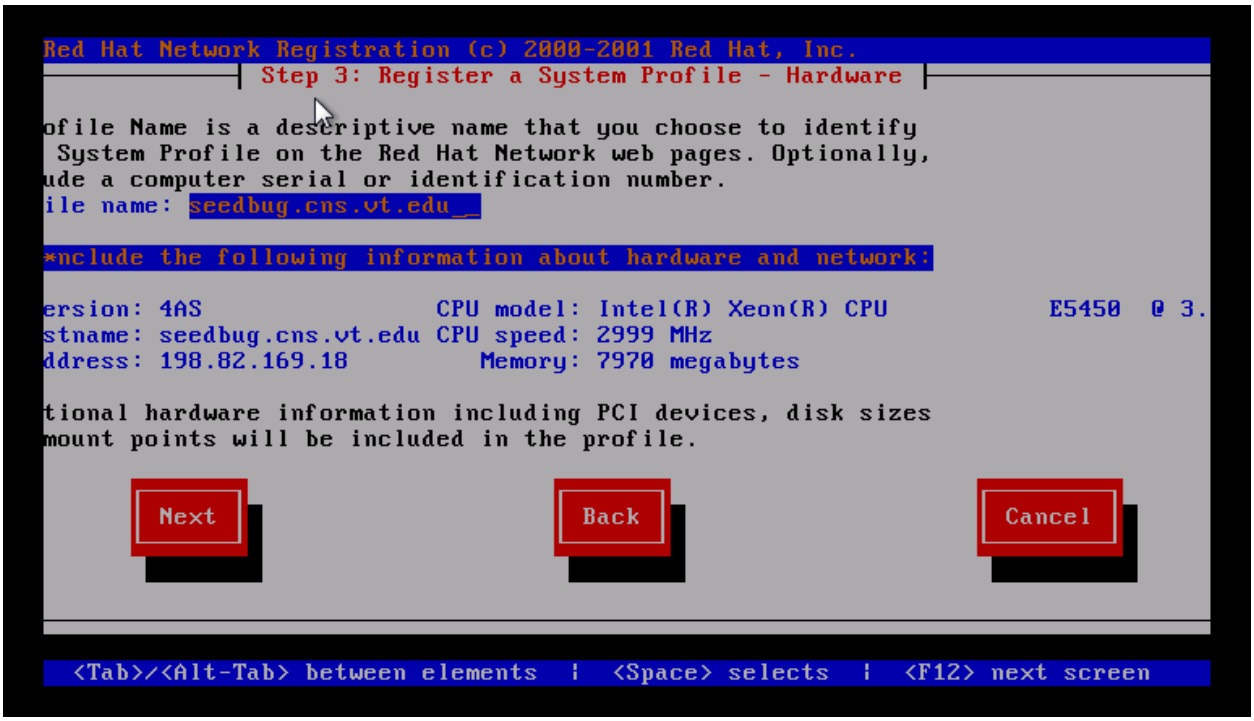
The Red Hat Network Registration initial page will appear. Read the text before continuing. Use the up-arrow on the keyboard to move the cursor from the "Next" box to the text field, then use the down-arrow on the keyboard to scroll through the text. Once the text has been read make sure "Next" is highlighted as above. If not, use the <TAB> key to cycle through the choices until the "Next" box is highlighted. <Enter> or <F12> will take you to the next screen.



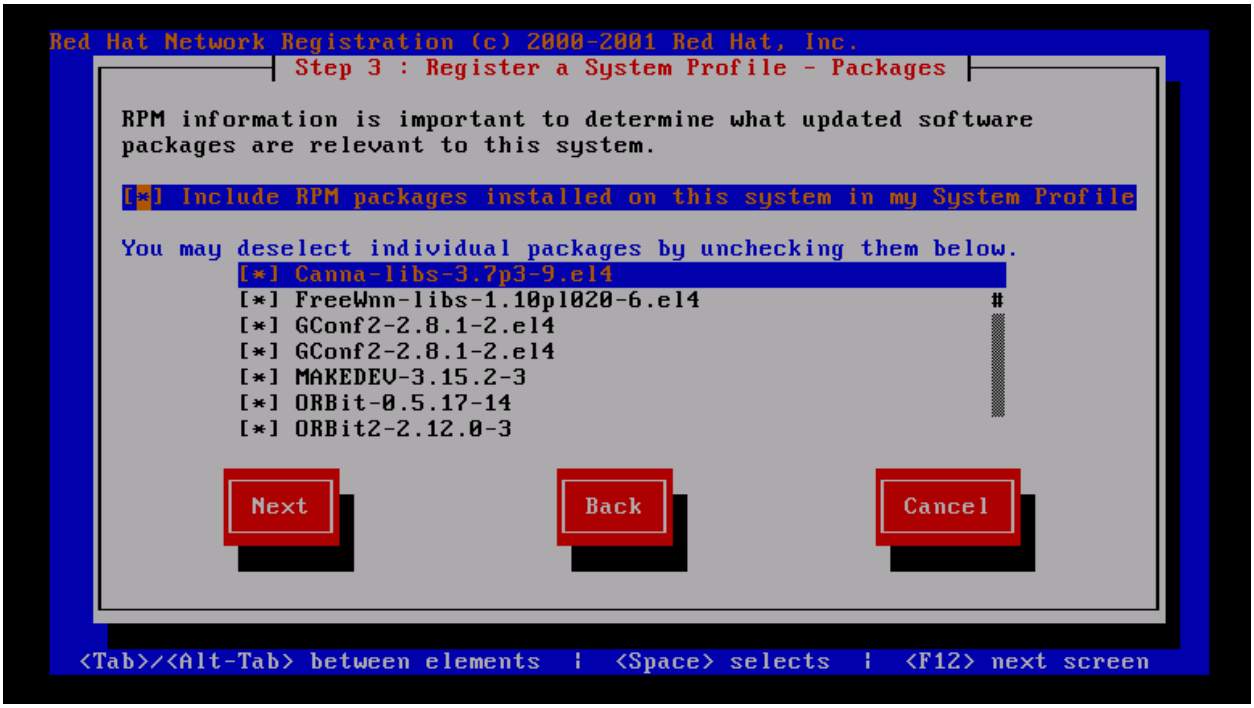
The next (second) screen is the privacy statement, which should be read in the same fashion, then continue to the third screen. You will need your Red Hat Network user name and password for this. The cursor should be in the "Red Hat Login:" box. Enter your Red Hat Network user id and password, using the <TAB> key to move between the fields. Then <TAB> to the "next" box to continue and hit the <ENTER> or <F12> key.



The next screen doesn't always display nicely. It shows a summary of the machine being registered. By default, the profile name is the fully-qualified system name. This can be changed to any text, but make sure there is some correlation between the profile name and the system name or function.



Once satisfied, go on to the next screen by <TAB>ing to the "Next" box and hitting the <ENTER> or <F12> key. The next screen shows a list of the RPM packages that are installed. Red Hat needs to know what packages are installed or they will not be updated. Software in the list may be deselected by using the up-arrow or down-arrow to select a package and the <SPACE> key to deselect (or reselect) individual packages. Most times no changes are made.



TO go on, <TAB> to the "Next" box and hit <ENTER> or <F12>. The next screen is a confirmation that all information has been collected. To actually send the data, <TAB> to the "Next" box and hit <ENTER> or <F12>. Once the data is sent, the finish screen will appear; hit <ENTER> or <F12> to go back to the root prompt. Now that the system is registered, it must be patched and usually rebooted.

For RHEL versions up to v.4, the up2date command is used, and kernel packages are not updated/installed by default. The most important options to the up2date command are --nox (no X), --list (list packages that have updates), --download (download only), --update (install the updates) and --force (to force updates to packages that are marked "skip" like the kernel packages). It's always a good idea to list the packages that will be upgraded before actually installing them. To list, at the command line prompt type

```
up2date --nox --list
```

which will generate the list of upgradeable packages.

All installed packages should be updated right after an install. To update all the packages, including the kernel:

[No screenshot until I actually patch a machine --lat]

For RHEL version v.5, the yum command is used, and kernel packages ***are*** installed/updated by default. The most important yum options at this point are check-update (check for updates) and update (perform the update). As stated above it's always a good idea to list the packages that will be upgraded before the actual installation. To list, at the command line prompt type

```
yum check-update
```

which will generate the list of upgradeable packages.

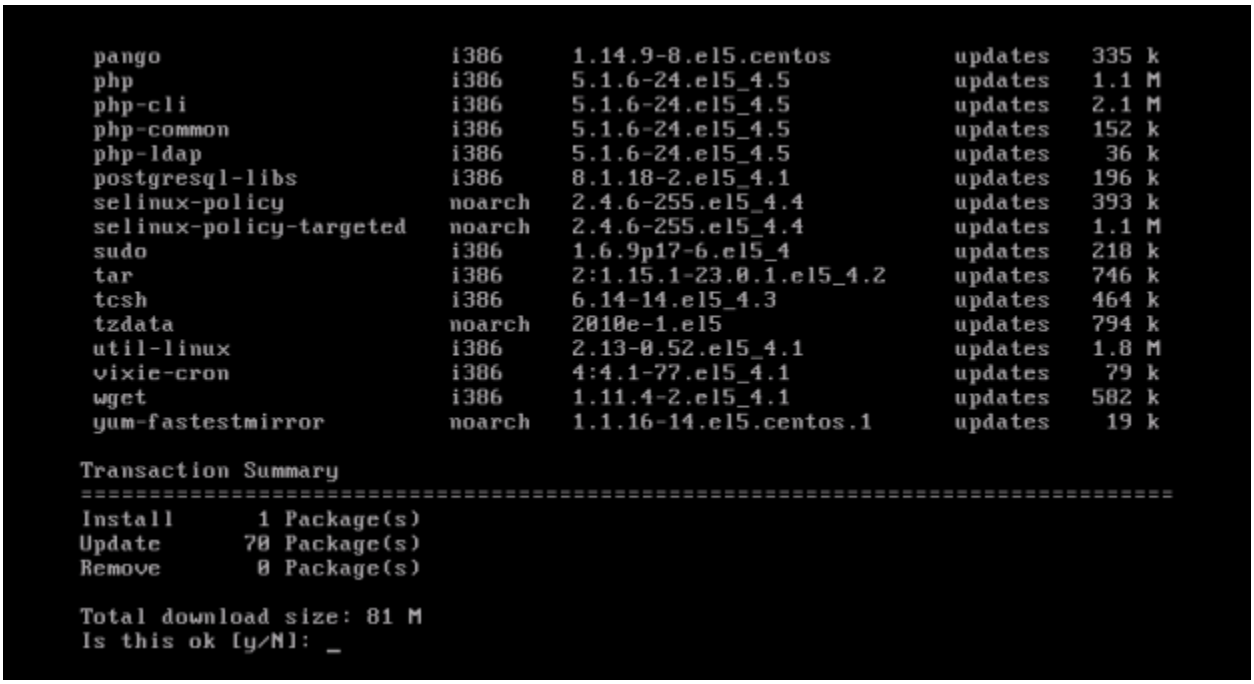
Once again, all installed packages should be updated immediately after an installation. To update all the packages on a RHEL v.5 system:

[No screenshot until I actually patch a machine --lat]

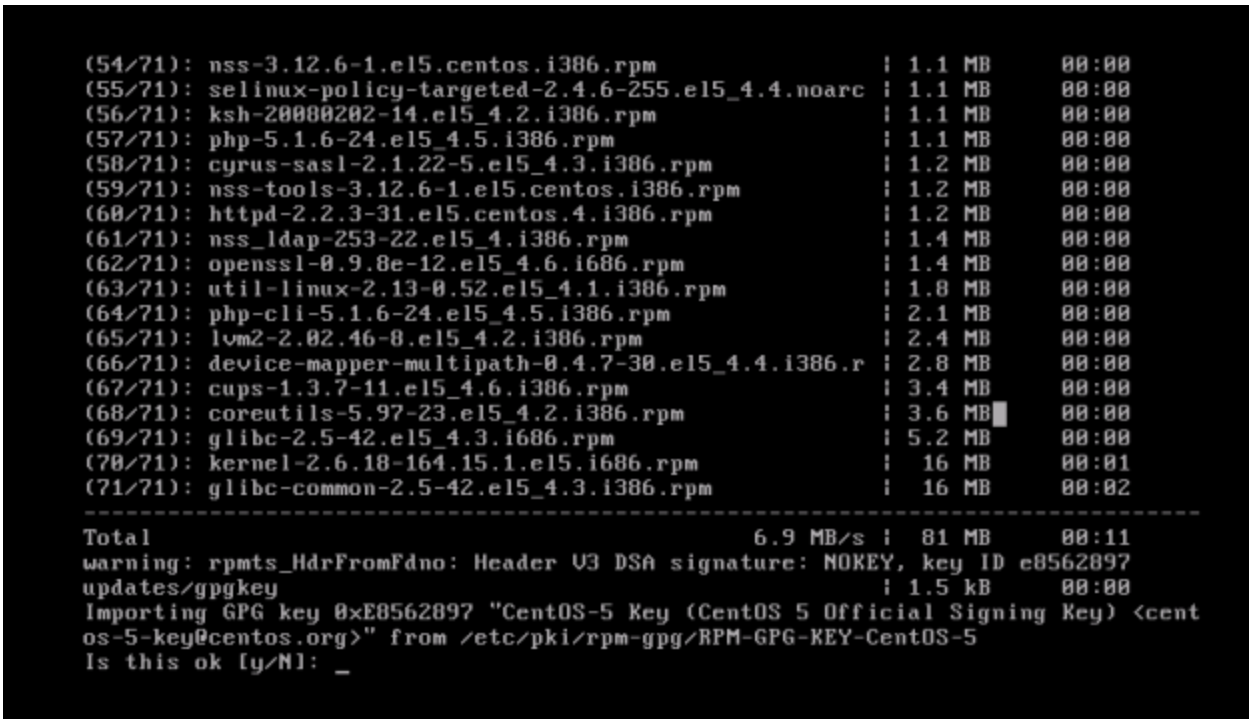
Once the machine is patched it should be rebooted to insure all patches are properly applied.

Note: RedHat has a different update system than CentOS. Someone with a current RHEL subscription should extend this section.

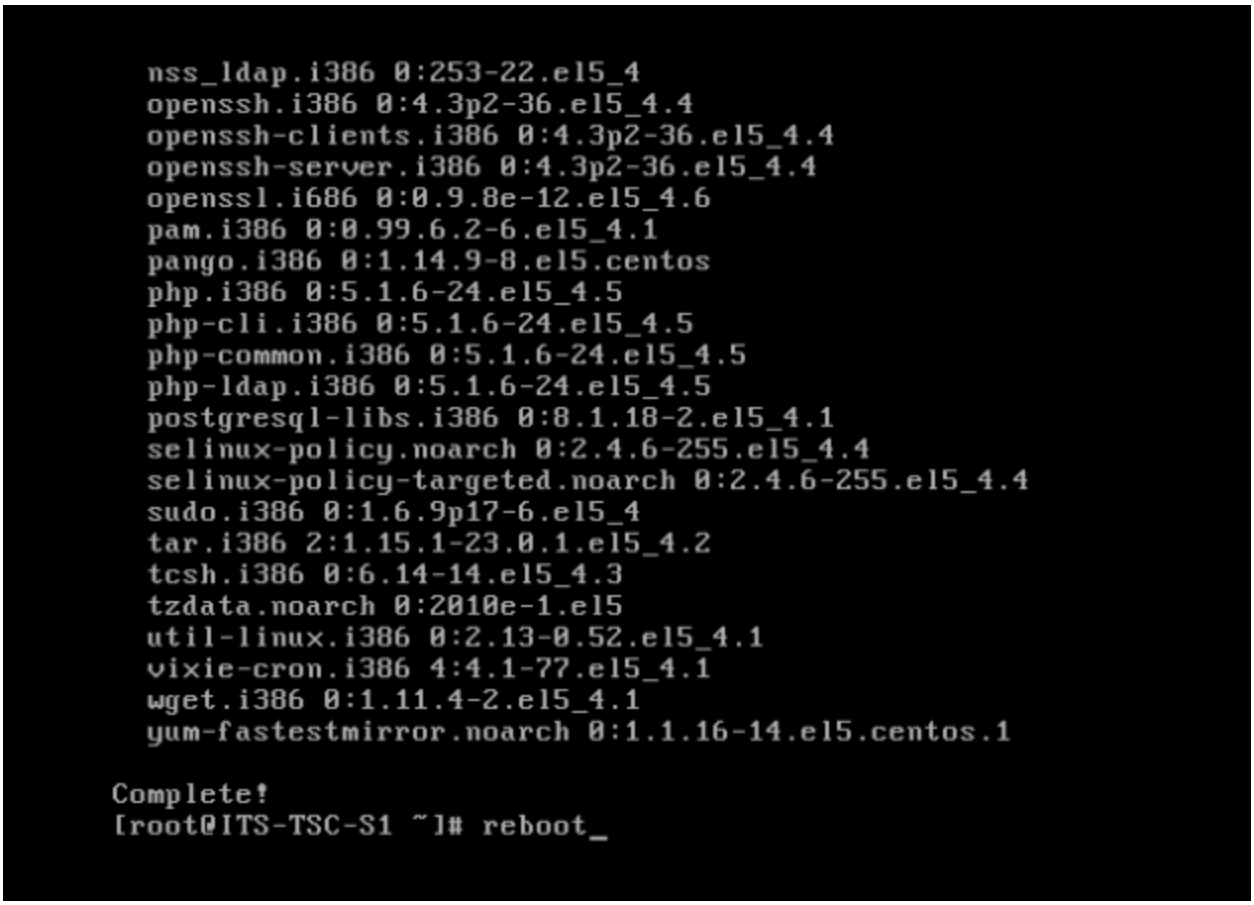
[Leaving the rest of this on patching in until real screenshots inserted].



It will ask your permission to continue after it checks to see what needs updated. Choose y and hit the Enter key.



In some cases you will get this warning letting you know there is a new GPG key for CentOS. Do not blindly accept keys. The CentOS Official Signing Key is OK, but other, less trusted repositories may not be. Be aware of what you are doing and the ramifications. For this example, we will choose y and hit enter in this situation.



After the updates have installed it will say Complete! And put you back at your root prompt. You should reboot the system once again to ensure that all of the updates are applied.

Securing With IP Tables

The host-based firewall that is bundled with RHEL and CentOS is IPTables. IPTables runs within the kernel and controls traffic flowing into and out of the server. For this guide, we only look at blocking incoming traffic, as if an attacker gains root-level access on the server, they can disable the firewall entirely.

TODO: put in examples for common IPTables configurations:

- Protect web server (HTTP, HTTPS, limit SSH)
- Protect email server (SMTP, POPS, IMAPS, limited SSH)
- Protect internal file server (Samba, limited SSH, CUPS)

Security With SELinux

Explanation here as to how SELinux works and how to resolve common problems.

Securing Apache

Pointer to the SANS document on securing web services

Securing FTP

Paragraph on how VSFTPD works

Suggestion to move to ProFTPD if extended security restrictions are needed

Securing Samba

Overview of Samba and how to use it in different configurations

Third Party Extras

Fundamentally, Linux distributions are a tradeoff. You could build everything yourself and get a system tuned completely to your needs. However, that takes time and a fair amount of management. If you wish to trade some of your customization ability to simplify management, distributions offer this. In order to do this, and to provide reasonable support, the company in charge of the distro must make decisions as to what is in or out of their particular "flavor" of Linux. In general, this works fine. Sometimes, though, it doesn't.

That's where third party repositories (repos) come in. These repos are not maintained by the company (Red Hat, in this case), but are maintained by the community. If you use one, you are undoing a portion of the tradeoff above. You are gaining customization at the cost of simple management and, sometimes, security. Simply put, Red Hat doesn't test their updates against those in the repos, so applying an update might break something... though it's unlikely. Third part repos also often do not have as deep a set of tests for new package versions and may not stay on top of security issues as the primary update repositories. However, in almost all cases, installing a package from a trusted repository is better than just downloading the package and installing it. If you use a repository, you can get security updates. If you just download the package, you have to track it manually. This is often forgotten and therefore results in exploitation.

Of course, like all of security, this isn't an all-or-nothing deal. In many cases, you can get highly customizable packages with a minimal lost of security and management. For a lot of businesses, this is a no-brainer, especially if the third party repository provides software that the business needs.

There are three commonly used repos for Red Hat Linux.

1) CentOS Extras

CentOS is a clone of Red Hat that is "binary complete". This means that running CentOS is almost identical to running Red Hat. You don't get the same logos or paid support, but if you don't need that, CentOS makes a lot of sense. The CentOS community has provided a few packages that they feel makes running their systems easier. This repo is enabled by default, so you can install a few more packages than Red Hat offers by default. Of course, there is nothing preventing you from adding the CentOS Extras repository to a standard CentOS box.

2) CentOS Plus

If you wish to upgrade specific packages over what Red Hat (and therefore CentOS) provides, you can use the CentOS Plus repository. This repo is NOT enabled by default, and has a higher chance of causing problems if you try to add it to an official Red Hat system. More information is available at http://wiki.centos.org/AdditionalResources/Repositories/CentOSPlus

3) RPMForge

RPMForge is a collaborative repository intended to extend Red Hat or CentOS. It is recommended that you first load CentOS Extras, so you can use the yum-priorities system to make sure that this third party repo is handled properly when it comes to package dependency resolution. More information is available at http://wiki.centos.org/AdditionalResources/Repositories/RPMForge

Last Updated: May 19th, 2019

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
SANS London June 2019	London, GB	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Zurich June 2019	Zurich, CH	Jun 03, 2019 - Jun 08, 2019	Live Event
Enterprise Defense Summit & Training 2019	Redondo Beach, CAUS	Jun 03, 2019 - Jun 10, 2019	Live Event
SANS Kansas City 2019	Kansas City, MOUS	Jun 10, 2019 - Jun 15, 2019	Live Event
SANS SEC440 Oslo June 2019	Oslo, NO	Jun 11, 2019 - Jun 12, 2019	Live Event
SANSFIRE 2019	Washington, DCUS	Jun 15, 2019 - Jun 22, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Cyber Defence Singapore 2019	Singapore, SG	Jul 08, 2019 - Jul 20, 2019	Live Event
SEC450 Security Ops-Analysis Beta 1	Crystal City, VAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Charlotte 2019	Charlotte, NCUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Pittsburgh 2019	Pittsburgh, PAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS London July 2019	London, GB	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Columbia 2019	Columbia, MDUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Rocky Mountain 2019	Denver, COUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS San Francisco Summer 2019	San Francisco, CAUS	Jul 22, 2019 - Jul 27, 2019	Live Event
SANS Pen Test Hackfest Europe 2019	Berlin, DE	Jul 22, 2019 - Jul 28, 2019	Live Event
DFIR Summit & Training 2019	Austin, TXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS Riyadh July 2019	Riyadh, SA	Jul 27, 2019 - Aug 01, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Autumn Sydney 2019	OnlineAU	May 20, 2019 - May 25, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced