Global Information Assurance Certification Paper

"Securing the Drake"

A
Tutorial on Securing
Mandrake Linux v8.1
and
Apache Web Server

GCUX v1.7

*By **Sam Clayton***

December 07, 2001

Purpose

The goal of this step-by-step documentation is to provide instructions on how to configure a secure public Apache web server using Mandrake Linux version 8.1. Securing this server will be accomplished using only the tools bundled with the Mandrake Linux three (3) CD set.

Hardware Specifications

- Processor: 1400 Mhz AMD x86 processor
- Random Access Memory (RAM): 512 MB PC133 SDRAM
- Hard disk: Seagate Barracuda 20 GB with 5400 rpm
- External Storage: Iomega Peerless Storage 20GB USB
- CD: Sony 16X CD ROM
- Network Interface Card: 3Com 10/100 OfficeConnect
- Video Card: Matrox Millennium G200 (AGP) with 16 MB SDRAM
- Mouse Type: Microsoft Optical (PS/2)
- Keyboard: Standard US 101 keys

Expected Results

Upon completing this tutorial, you should have a better understanding of the Mandrake Linux version 8.1 operating system. More significantly, you will have a secure public Apache web server that is able to handle typical Internet traffic over TCP (transmission control protocol) port 80 (HTTP), and encrypted traffic using secure sockets layer (SSL) over TCP port 443 (HTTPS). SSL will use PKI (public key infrastructure) certificates using triple DES encryption. The finished product will be a web server that only responds to HTTP or HTTPS connections.

Tutorial Outline

1. Installing the Operating System
2. Securing the Operating System
3. Securing the Web Server
4. System Administration

Summation of Responsibility

In many network architectures, the publicly accessible web server is viewed as the most vulnerable server. Due to its high visibility on the Internet, a web server can create security issues, by putting the machines around it at risk. It can also be a form of embarrassment if the index (home) page of your web site is defaced. However, many companies are willing to take that risk because of all the money that can be made on the Internet. Adding the great security issues and the significant financial gains that can be made with a web server together gives you an idea of how secure the system needs to be. The level of security should always be directly proportional to the value of the information and/or level of damage that can be caused if compromised.

That being said, it is necessary to examine the security issues that will need to be addressed when securing a web server. Some of the security concerns and threats include denial of service attacks, buffer overflow attacks, malicious code (CGI scripts, JavaScript), directory listings, incorrectly configured settings, server performance, and unwanted active services, to name a few. These are just of few of the obstacles that must be overcome in order to provide a secure Internet worthy public web server.

1. Installing the Operating System

1.1 Basic Input / Output System (BIOS) Configuration

The BIOS is a software application stored in the read-only memory (ROM) of the system board (also known as the motherboard). For this reason, some refer to the BIOS as ROM BIOS or firmware. The BIOS is responsible for running the power-on self-test (POST), initiating the loading of the operating system (OS) into the random-access memory (RAM), running the System Setup program, and facilitating communication between the central processing unit (also called the CPU or processor) and system hardware components.

To briefly explain a few of these terms, the POST simply executes a functional check of the basic system devices such as the keyboard, mouse, monitor, floppy drive, etc. A successful error-free check of these basic system components is indicated by one beep during the computer boot or startup. The System Setup program gives the computer user access to the Complementary Metal-Oxide Semiconductor (CMOS). The CMOS contains hardware configuration settings and is located on the battery powered real-time clock (RTC) chip. The CMOS is accessed in various methods depending on the BIOS version and brand. Pressing the “Delete”, “F1”, or “Esc” keys during startup accesses many CMOS applications. Usually there will be a message on the screen that will tell you what button or buttons to push to enter the setup. Try to enter your CMOS.

When you enter your CMOS application look for the option that lets you indicate whether the operating system (OS) installed or being installed is a “plug and play” OS. For example, the “plug and play” option on my computer is located under “PNP/PCI Configuration” and the actual option says “PnP OS Installed”. If I had Windows 95 or greater (not including the Windows NT OS series) installed on my computer I would choose “Yes”, because this tells the BIOS that Windows will be initializing my hardware components. However, for GNU/Linux this setting needs to be set to “No”. Doing this will allow the BIOS to initialize your hardware components, in order to help GNU/Linux recognize some of the devices in your computer it may not be able to initialize.

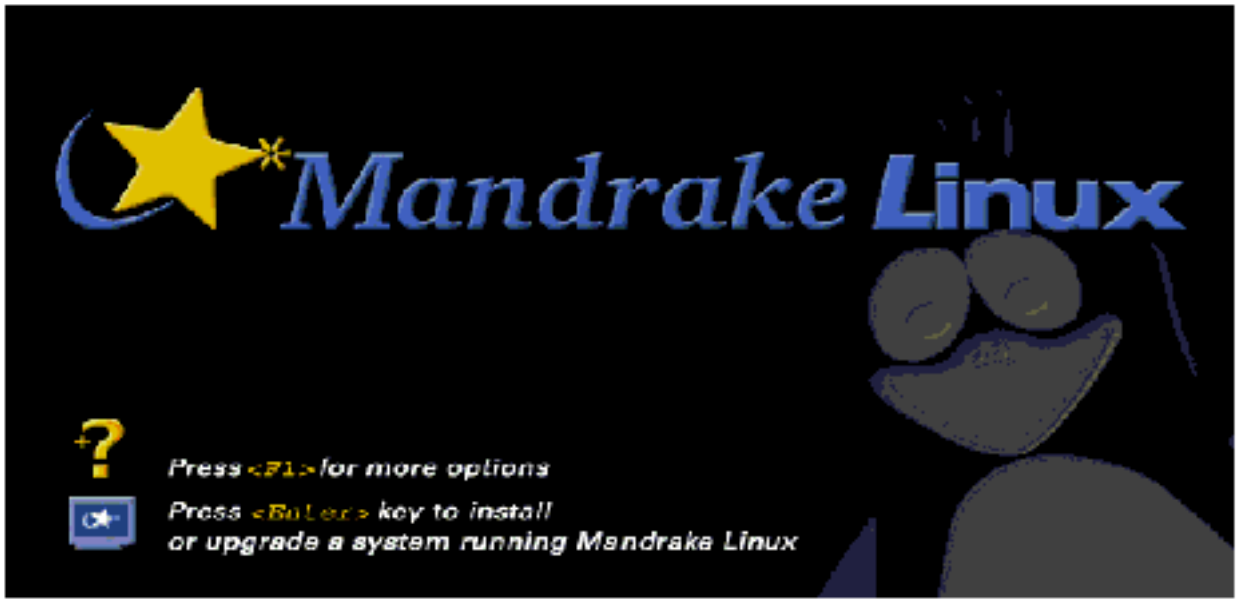
Assuming your machine has the functionality to boot from CD-ROM, while you are in the CMOS System Setup, make sure that your system is configured to boot from the CD-ROM for installation. This can be accomplished by looking for the “Boot Sequence” option in your CMOS and configuring your boot sequence option to boot from the CD-ROM first. This will make sure that the system does not try to boot from the floppy drive or the hard disk if there is already another OS running on your system. If you are

running another operating system off the same hard disk, it is strongly recommended that you backup your system before starting this installation. Installing this operating system may require re-partitioning the hard disk and data could be lost.

When all the aforementioned configuration changes have be completed, remember to save the changes on exit. Be sure to read the CMOS exit message carefully, because they are often worded awkwardly.

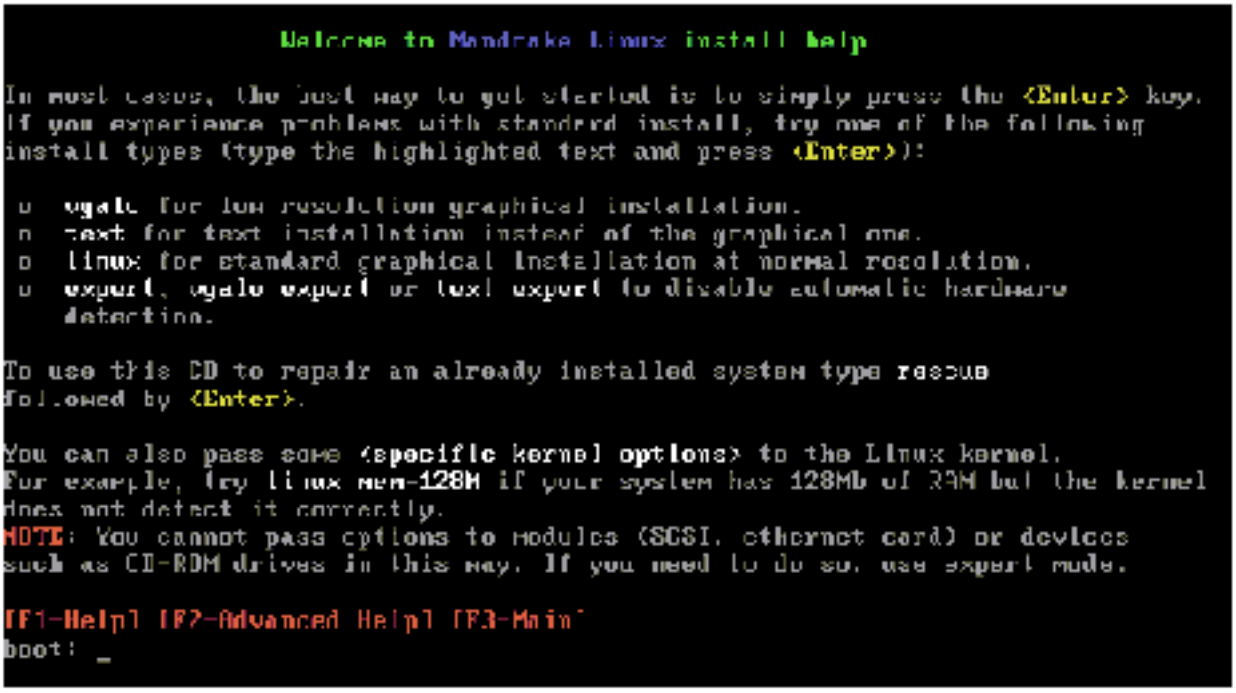
1.2 Begin Installation Application

Now that your machine has a properly configured BIOS and the CMOS has been configured to boot from the CD-ROM you can start the actual operating system installation of Mandrake Linux. Of course, the installation begins by putting CD 1 of the three Mandrake installation CD's into the CD-ROM drive, and beginning the boot process by restarting your computer. The first screen that appears when beginning your installation can be seen below.



(Image from Mandrake Linux User's Guide)

On this screen you have the option of pressing the <F1>, or <Enter> buttons on your keyboard. If you press neither of these buttons, or if you press the <Enter> button, the default installation process will begin. Pressing the <F1> button will take you to an installation help and options pages. From this page, several installation options can be performed based on your level of experience with Linux or based on any problems you may have encountered with a previous installation of Linux. The next page shows a screenshot of the options panel.



(Image from Mandrake Linux User's Guide)

Following is a brief explanation of what each installation option is used for:

- vgalo. This option will present each installation screen in low graphic resolution. This option is often used when the graphical screens for a normal installation do not display properly. A problem such as this could be caused if your video card is very old and not recognized by Linux or your BIOS.
- text. The "text" option will present the entire installation in text mode. A true command-line programmer may prefer this option. If using the "vgalo" option does not solve the graphical installation problems that you may be experiencing, then this "text" option can be used to facilitate your installation.
- linux. The "linux" option is the default option. This is the option that is used when you press <Enter> on the first installation screen, seen above. This installation mode is also initiated when neither the <F1>, nor <Enter> buttons are pressed on the first screen. This mode provides a graphical installation in normal resolution (most likely 800x600).
- expert. The "expert" option can be used by itself or in conjunction with the "vgalo", "text", or "linux" options to prevent hardware components from being detected automatically. This option can be used in instances where permitting automatic hardware detection causes your computer to freeze. Installing Linux with this option should keep your computer from freezing, however, this option does require you to provide the hardware parameters by hand.
- vgahi. Using the "vgahi" option will run the graphical installation in high resolution. This mode can be used when you are sure that GNU/Linux will recognize the video card you are using.

- vga16. This option can also be used to remedy graphical problems that may have occurred during a normal or high-resolution installation. This option presents a graphical installation with 16 colors and a resolution of 640x480.

Command-line options can also be added to the installation options. These command-line options are passed to the installation kernel. An example of a command-line option is the mem=xxxM command, where xxx is the number representing the amount of RAM installed on the motherboard. This command can be used when the installation program is unable to recognize the amount of RAM installed on the motherboard. This command is executed by simply adding it after your installation option selection. See below:

boot: linux mem=320M

This tells the installation kernel that your machine has 320 megabytes (MB) of RAM installed.

By pressing the <F2> button on your keyboard, you can view the "Advanced Help" options. This page contains information on the "vga16" and "vgahi" installation options. In the middle of the page, information on additional command-line options can be found. You can use these options, if necessary, to help refine the installation you require. For example, if you have already partitioned your disk or if there is another OS on the same disk, you may not want Linux to attempt to repartition you hard disk. In this case you would use the "readonly=1" option for your installation selection. Another option that may be of interest is the "noauto" option. This option does the same thing as selecting the "expert" installation in that it disables the Linux hardware auto-detection feature. However, adding this option to your installation will require you to provide the hardware parameters by hand.

If you require additional commands for your installation, this page contains a few more commands. These commands and their function are below:

- display=ackbar:0. Use this command to export the installation display to the "ackbar" machine screen. In this command "ackbar" is the name of the machine. This should allow you perform a remote install.
- Security=n. In this command the security level can be set to a value of n, where n is a number from 0 to 5 (5 being the highest security level).
- updatemodules. This command requires a special update floppy disk containing module updates.
- patch. This command allows you to use a patch from a floppy disk with a file named "patch.pl".
- auto_install=floppy. Use this command to enable auto_install using auto_inst.cfg file on a floppy disk.

Now that you are aware of the various installation options and command-line options, you should be able to select an option that suites your purpose best. In most cases, simply pressing <Enter> on the first installation screen will suffice. If you require or

desire any of the different options explained earlier simply press the <F1> button and enter your installation option and command-line option (if any) on the bottom of the screen next the boot: prompt. To build this web server, I have chosen to start with the standard installation option with memory specification. Therefore, I have entered:

linux mem=320M

at the boot: prompt, and pressed <Enter>. When the installation begins the option to see the logs of the installation process and kernel logs are available. The button sequence needed to view these logs can be found at the bottom of screen once the installation begins. I pushed the <Alt + F3> buttons to see the installation log messages. This may be helpful if you would like to see some of the actions and applications that are being loaded to run the installation option you selected at the boot: prompt.

The next screen that will appears that requires you to provide input is the “Choose Your Language” screen. While this screen is trivial with regard to input, it is important that you understand the layout of this and any remaining installation screens. The menu on the left indicates your location with regard to installation steps. Of course, on this screen you are at the very top of the installation process. Your location is indicated by the color of the star next to the title of each installation step. See the screenshot below.

(Image from Mandrake Linux User's Guide)

A red star indicates that the step has yet to be completed, an orange star indicates the current step you are on, and a green star indicates that the step has been completed. If you choose to go back to a previous step, you may do so by using your mouse pointer to click on the star corresponding to that step. Depending on the progress of your installation some steps may not be available. If a step is available, the star corresponding to that step will be highlighted when the mouse pointer is moved over it.

Located to the right of the menu, is the input and information part of each installation screen. The upper portion of the screen is where you will enter any requested information or make your selections. The lower portion provides additional information to help you with the selection process. The information in this lower section will also explain some of the advanced features of the selection options.

After you have chosen your language and accepted the terms of the license, you are prompted to select an installation class. Because I want to customize this installation, I select "Expert" at the prompt. There are many benefits to this type of installation. The "Expert" installation option is preferred because it allows you to be specific about how you would like your system to be configured. This flexibility will allow you to eliminate the installation of unnecessary services (daemons) and applications that may compromise the security of the system and hinder its ability to fulfill its purpose. Many options that are not available through the "Recommended" installation are available through the "Expert" installation. To further elaborate on the benefits of an "Expert" installation, an indication note will preface all options not available through the "Recommended" installation. Finally, since this is a new installation on a new hard disk I chose to install as opposed to update. A picture of this screen can be viewed on the next page.

(Image from Mandrake Linux User's Guide)

1.3 Disk Detection and Configuration

(Note: This option is not available in the Recommended installation option.)
The next step you will encounter once you have decided on your installation option is "Hard drive detection". In this part of the installation your hard disk(s) and any SCSI devices are detected. You will be prompted during the installation to confirm the existence of SCSI interfaces. Simply answer this question based on your system hardware components. If you have a SCSI interface installed select "Yes" else select "No", then click "OK". If you are unsure select "See hardware info", then click "OK" to view a list of the hardware that was recognized by Linux. Since there are no SCSI devices in my machine, I have selected "No".

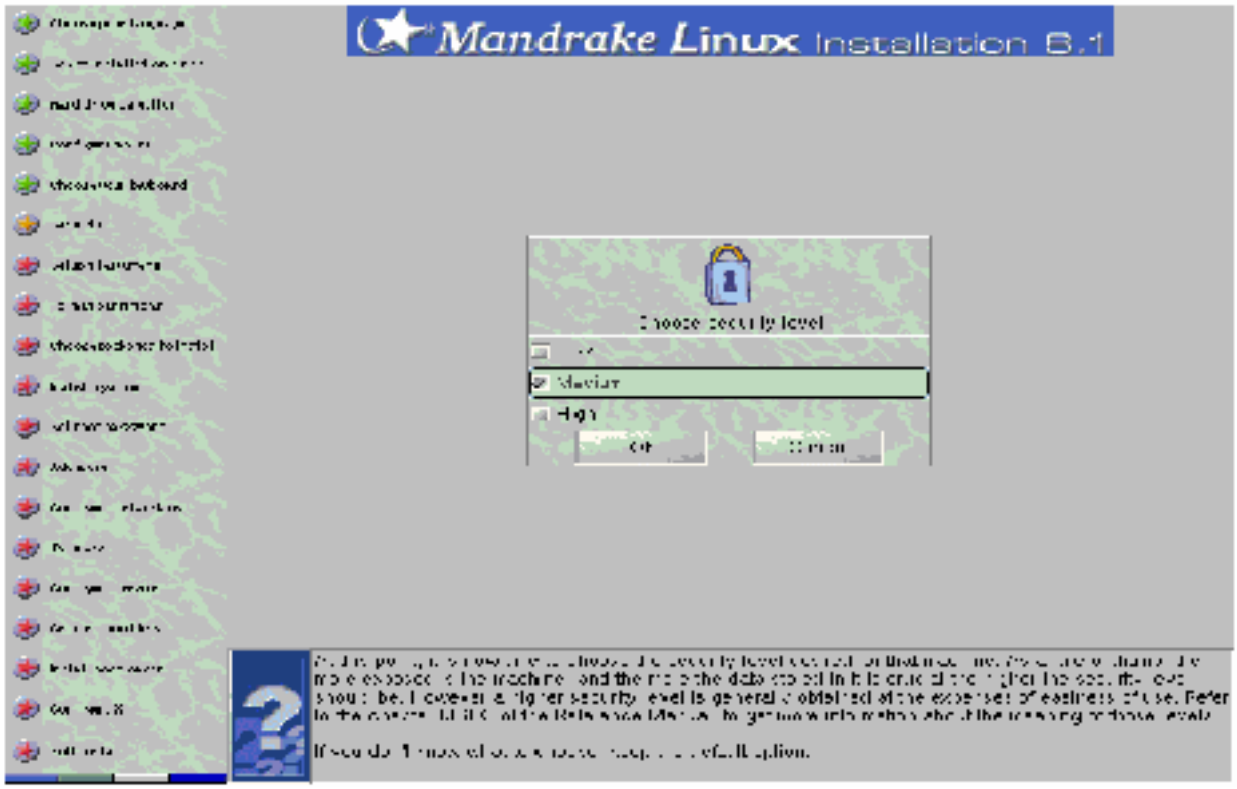
1.4 Mouse Configuration

(Note: This option is not available in the Recommended installation option.)
The mouse configuration step, while seeming to be a very trivial configuration may cause a problem for some. The installation program will recognize whether you have a PS/2, USB, or serial mouse, however, it may not select the correct mouse type for that category. For example, I am using a PS/2 optical mouse with wheel, but the installation program selected a PS/2 Standard mouse. To correct that selection I double clicked on the Generic PS/2 Wheel Mouse option. The installation then takes you to a test screen

to determine, if the mouse setting you have chosen is correct. Initially, the mouse did not work correctly. However, by chance I persisted and the mouse buttons and wheel began to correspond with the mouse illustration on the test screen. This may cause a problem if you get discouraged too quickly and decide that the option you selected was incorrect. In my first installation of Mandrake Linux, I ended up selecting the default mouse option after running into this problem. I then had to restart the entire installation because my mouse was configured improperly and would not move out of the corner of my monitor. Hopefully, this will not happen to you. If you decide to select a mouse other than the one that Linux selects for you, just remember to click around and move your mouse a little bit before deciding that you have chosen an incorrect mouse type.

1.5 Security

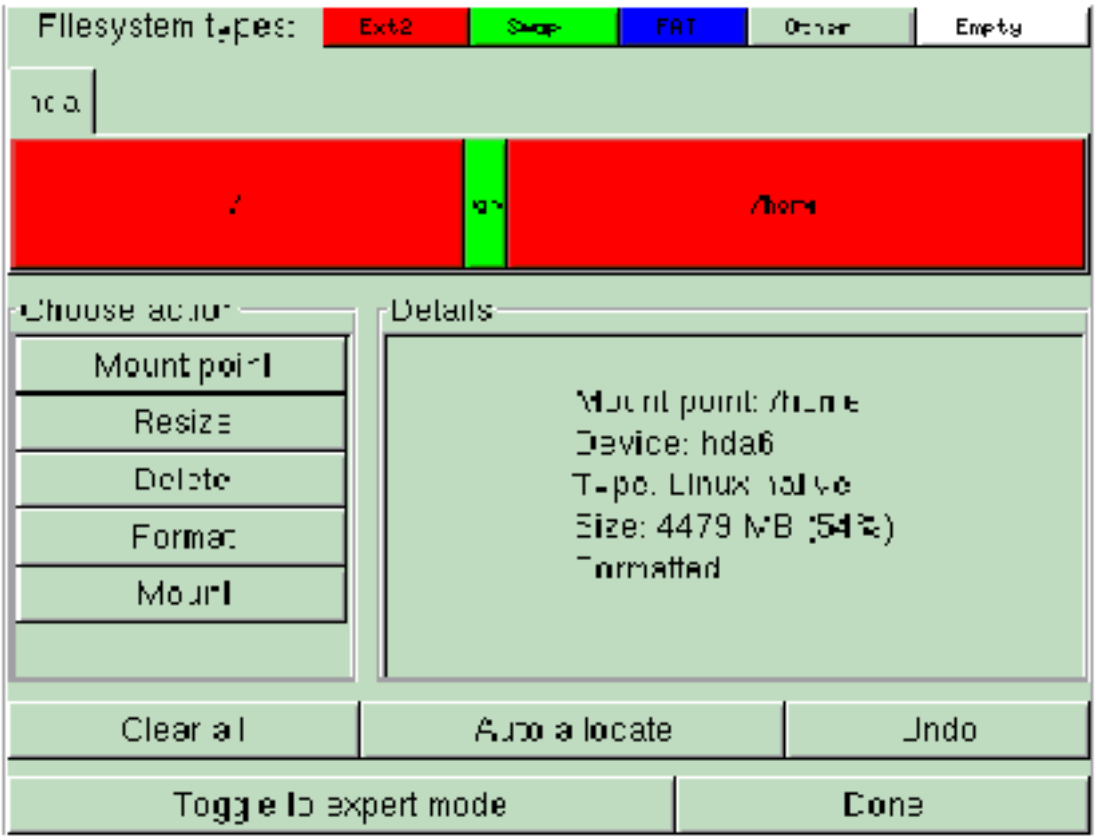
(Note: This option is not available in the Recommended installation option.)
After configuring your mouse and keyboard, you are presented with security options. You have three options to choose from – Low, Medium, and High. Because the purpose of this system requires it to be accessible from the Internet, I have selected the "High" security option. If this was simply going to be a workstation, the "Low" level security option may be sufficient. The "High" security level setting configures the computer to a state where the system can be used as a server. This means that security checks are run periodically, and the system is checked for open ports. At this level, the administrator is the only individual who can activate ports and grant connections to this machine from other computers. The screenshot below shows what this security selection panel looks like.



(Image from Mandrake Linux User's Guide)

1.6 Setup File Systems

(Note: This option is not available in the Recommended installation option.)
Now that you have selected your security level, you will have to setup your file systems using the DiskDrake application. The graphical interface for DiskDrake in Mandrake Linux 8.1 is similar to the screenshot below. The primary difference in the new 8.1 version of Mandrake is that this panel now includes a "Wizard" and a "More" button. If you would like to know what the other buttons do, simply read the text in the information window on the lower right side of the screen. For my installation I have DiskDrake set on "Expert mode", so the toggle option says "Toggle to normal mode" as opposed to what is shown on the screenshot.



(Image from Mandrake Linux User's Guide)

Selecting the "Wizard" will automatically create three partitions and then ask you which partition you would like to format. The three partitions that it creates are the root (/), swap, and home (/home) partitions. The downfall of this is that you are not able to resize these partitions unless you press "Cancel" before moving on to the formatting step. When you press "Cancel", you are presented with a screen similar to the one above, wherein you are able to resize the partitions made by the "Wizard".

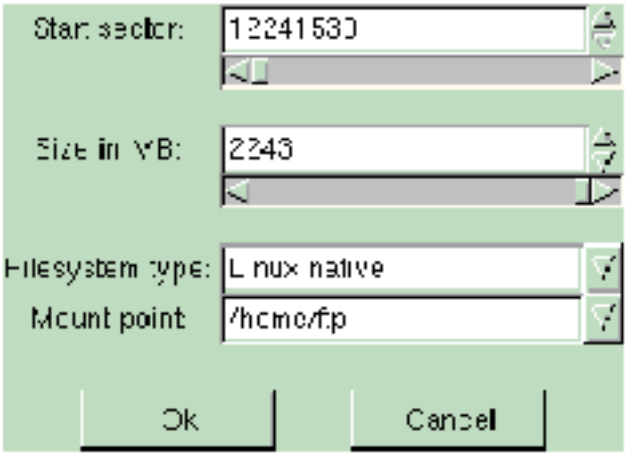
Selecting the "More" button will provide access to additional options such as:

- Save partition table
- Restore partition table

- Rescue partition table
- Reload partition table
- Removable media auto-mounting

Save Partition Table. This option allows you to save your partition table to a floppy disk. The floppy disk can be used later to restore or recover the partition table if necessary.
Restore Partition Table. Use this option to restore a partition table from a floppy disk.
Rescue Partition Table. Use this option to attempt a recovery of a damaged partition table.
Reload Partition Table. This option can be used when you want to undo any changes you have made to your partition table and reload your initial settings.
Removable media auto mounting. Use this option to auto mount your CD and floppy drives.

To accomplish the configuration of my file system I chose to create my partitions manually. This was done by clicking on the bar under "hda" as seen in the diagram on the previous page. Since I am using a brand new hard disk, the bar was colored all white to correspond with the "Empty" tab on the upper right corner of the DiskDrake panel. By clicking on the bar, a "Create" button appeared in the "Choose action" area. By clicking on the "Create" button, a new panel appears with options for defining a new partition. Ignore the "Start sector" option completely and simply adjust the size selector to your desired partition size. Select "Linux native" as your "Filesystem type" and name your mounting point accordingly. You should repeat this procedure for each partition. A screenshot of the partition definition panel can be seen below.



(Image from Mandrake Linux User's Guide)

Once you have completed configuring your partitions, it is a good idea to save your partition table. To do this click on the "More" button and select the "Save partition table" option. You will be prompted to insert a floppy disk and warned that any information on the disk will be lost. After you have completed all of your selections press "Done". Below is the list showing how I have partitioned my machine.

- / (root) – 1 gigabyte (GB)

- swap – 800 megabytes (MB)
- /usr – 3 GB
- /var/spool – 2 GB
- /var/log – 2 GB
- /http/docs – 2 GB
- /http/css – 2 GB
- /http/cgi – 2 GB
- /http/images – 2 GB
- /temp – 1.6 GB

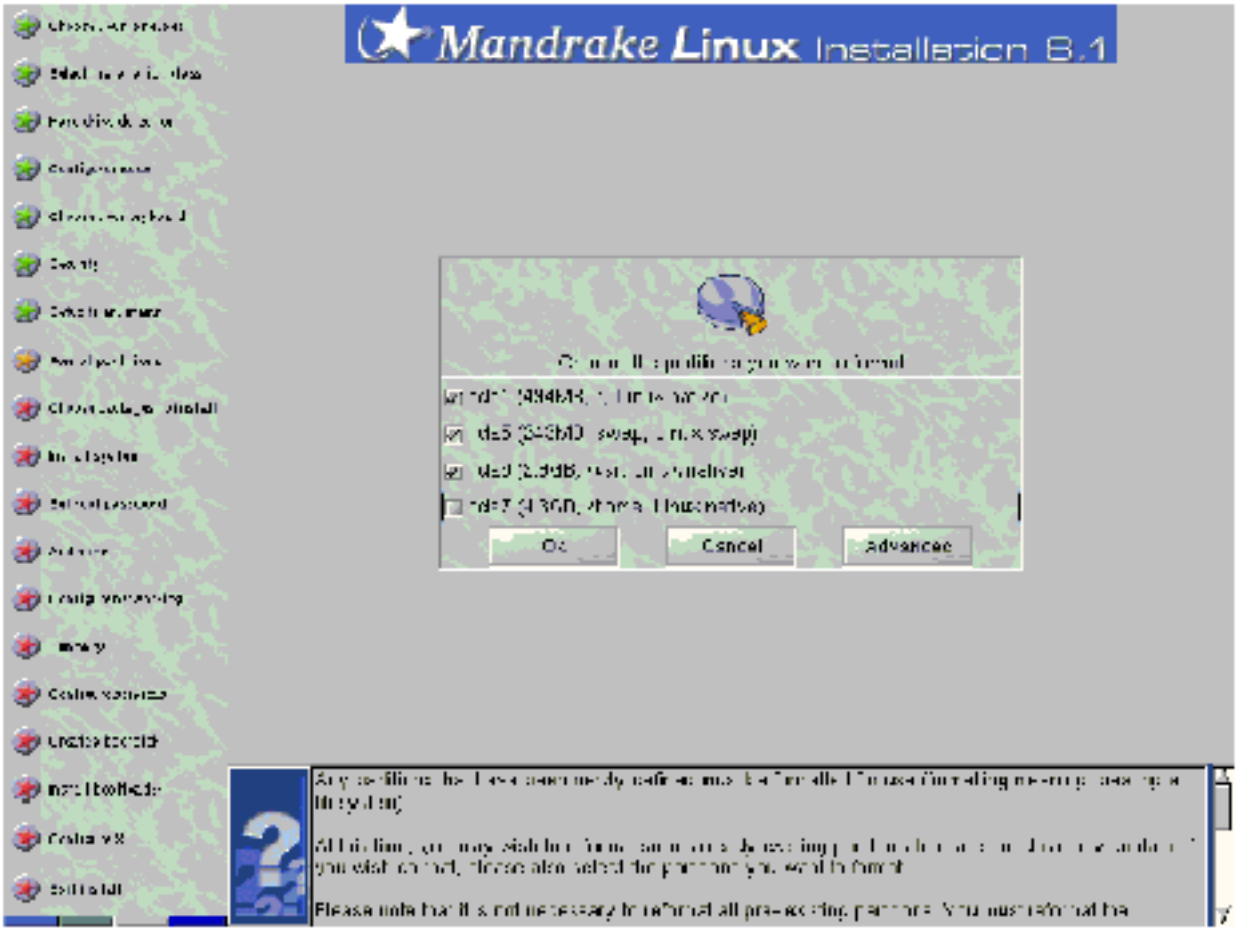
1.7 Choose Partitions to be Formatted

(Note: This option is not available in the Recommended installation option.)
You are then asked to select the partitions you want to have formatted. If you have a new drive like me select all partitions for formatting.

1.8 Choose Packages to Install

Finally, you have the option to install the packages that will truly define the role of your machine. Remember to only choose the packages necessary for this machine to carry out its role as a web server. Also, make sure to select the "Individual package selection" option at the bottom of the panel, this will allow you to deselect certain applications installed by default with certain packages. On the next page is a screenshot of the package selection panel. This panel does not reflect my selections nor should you have all of these items selected if you are building a web server. You can hover your mouse pointer over each package to get a brief explanation of the applications and / or accessories bundled with a particular package.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



(Image from Mandrake Linux User's Guide)

The list of packages to choose for a web server is as follows:

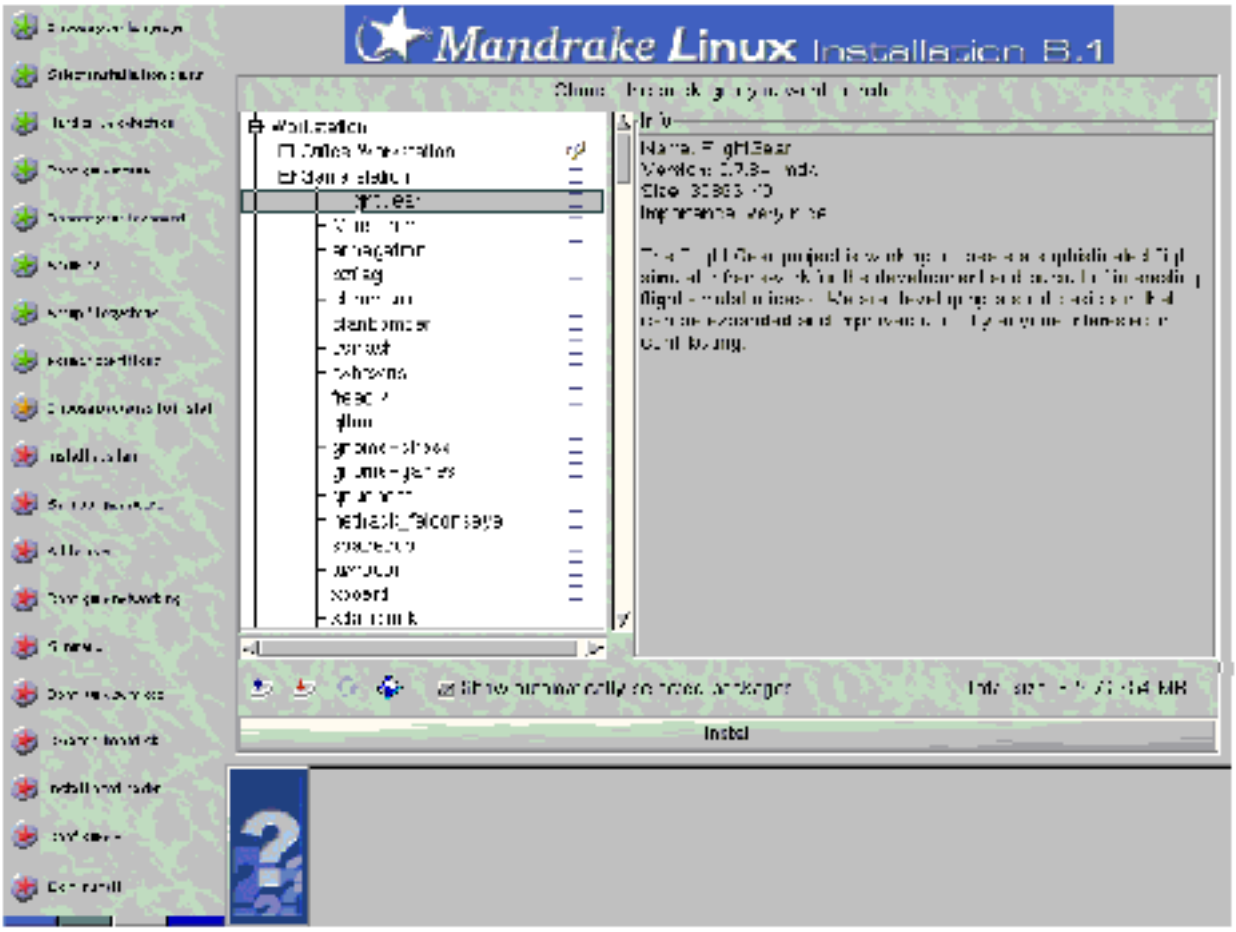
- Internet Station
- Configuration
- Development
- Documentation
- Web / FTP
- Firewall / Router
- KDE Workstation
- Gnome Workstation

Explanation
Internet Station. This package installs a web browser. Having a web browser on the machine will allow the web developer / administrator to make sure that any new content added to the server will display properly. This does not mean that this machine should be used for testing new software, or should it be used for casual web browsing. New software and applications should always be tested on a test machine in a test environment. However, to ensure that the new web documentation or software is behaving properly once installed on the production web server, it may be advisable to

have a web browser on the production web server. This will facilitate the examination of any new updates, by allowing the web developer to view changes on the server immediately after installation. For example, if your web server is located in a server room, and you only have access to that particular server, the only way to make sure that your updates are installed properly is to check how it displays through the web browser on the production server. If your update does not display correctly you are aware of it immediately and can take appropriate action. Without the browser installed on the server, you may not become aware of any problem until it is too late.
Configuration. This package installs configuration tools that can be used to provide additional server security.
Development. The development package installs programming languages such as C, C++, Python, PHP, and Perl. Since this web server will provide dynamic content it will be necessary to have these programming languages installed for CGI (common gateway interface) programming.
Documentation. This package installs How-To's and other documentation material on the operation system, configuration options, and tools. If a problem arises with the web server, this documentation could be useful in solving it quickly.
Web / FTP. Since this is slated to be a web server, this package was selected to install the Apache Web Server. On the "Individual package selection" screen, be sure to deselect all FTP services. FTP is not going to be used at all on this server, therefore there is no reason to have the application installed.
Firewall / Router. The Firewall / Router option should install the iptables and a few other tools that can be used to secure the server. The iptables will be used to create a host-based firewall that will block all ports and services other than those necessary for web traffic. The intention is to only permit access to the httpd service, and ports 80 and 443 for HTTP and HTTPS, respectively, for inbound connections only.
KDE Workstation. This package provides the basic graphical user interface for the Linux OS.
Gnome Workstation. This package provides more applications and desktop tools.

When you have finished selecting your packages, click "OK" to go to the "Individual package selection" panel. This panel has hundreds of different packets that can be installed on your system. Click on the "+" or "-" sign to expand and contract the trees. Check marks indicate a selected item. A clear check mark indicates that a sub-tree has some but not all options selected. A yellow check mark indicates that all items under a tree have been selected or that particular item has been selected. This is a painstaking process, but you must go to each checked item, read the description of the item that is checked, and determine whether you will need this as part of the installation. The description of each item can be read by simply clicking on the space between the package title and the corresponding check box. The description will give you an idea of the package's importance by reading the information after the "importance" label. In many instances you will be forced to keep packages that you do not want, and packages whose "importance" is listed as "very nice" or "nice" because it is linked to a package that is very important. Nonetheless, you want this machine to be as lean as possible, yet still able to accomplish its responsibility as a web server.

After reading the description for each of the selected items, use a floppy disk to save your package list. If you find that this is a good list of packages, you can use this list for future installations. Below is a screenshot of the "Individual package selection" screen.



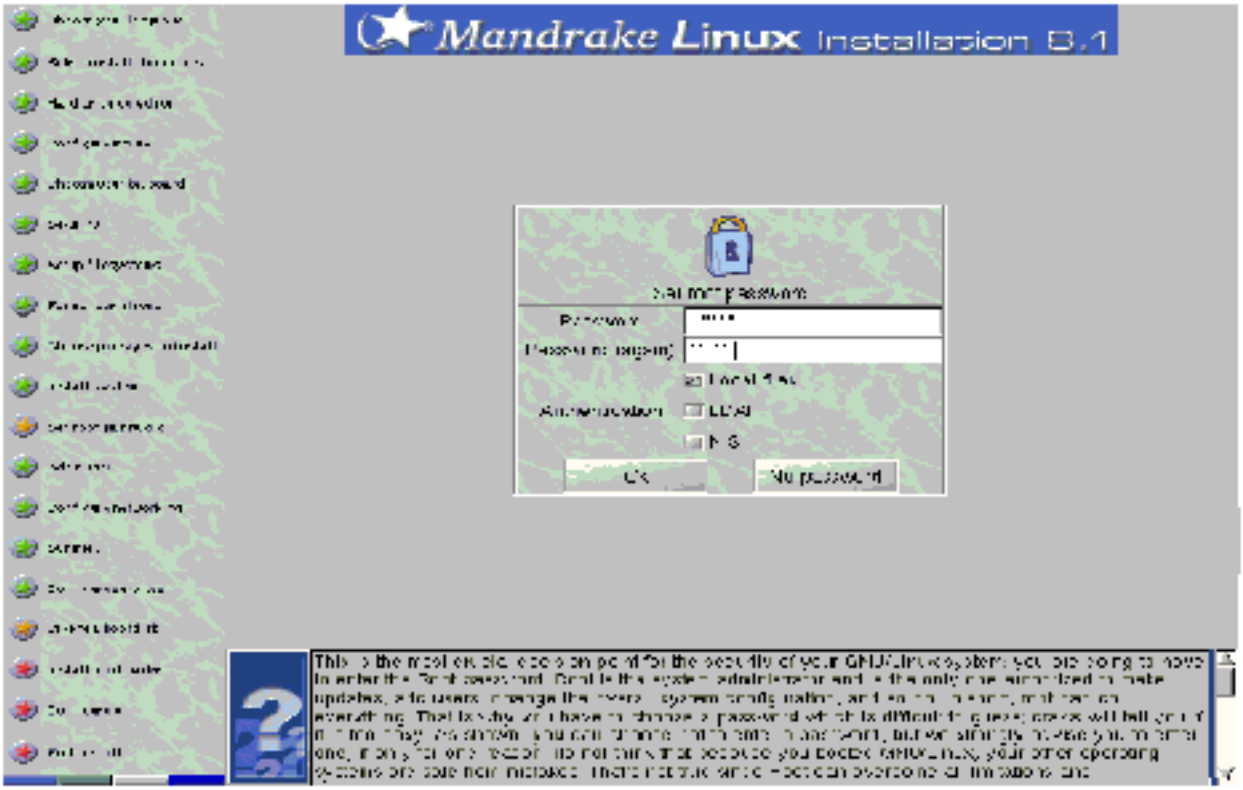
(Image from Mandrake Linux User's Guide)

The purpose of this screen is simply to show you what it looks like. None of the options selected on this screen is appropriate for a web server configuration. Finally, press the "Install" button. Since you have elected to install severs on your machine a message box will pop up warning you of the possible danger of running servers on your machine. This box will list all the servers that are going to be installed. Simply click "OK" if those are the servers that you want installed and the installation will begin. You can take this time to stretch your legs because the installation may take a while. You may also need to insert another installation disk into the CD-ROM, so do not go to far from your computer.

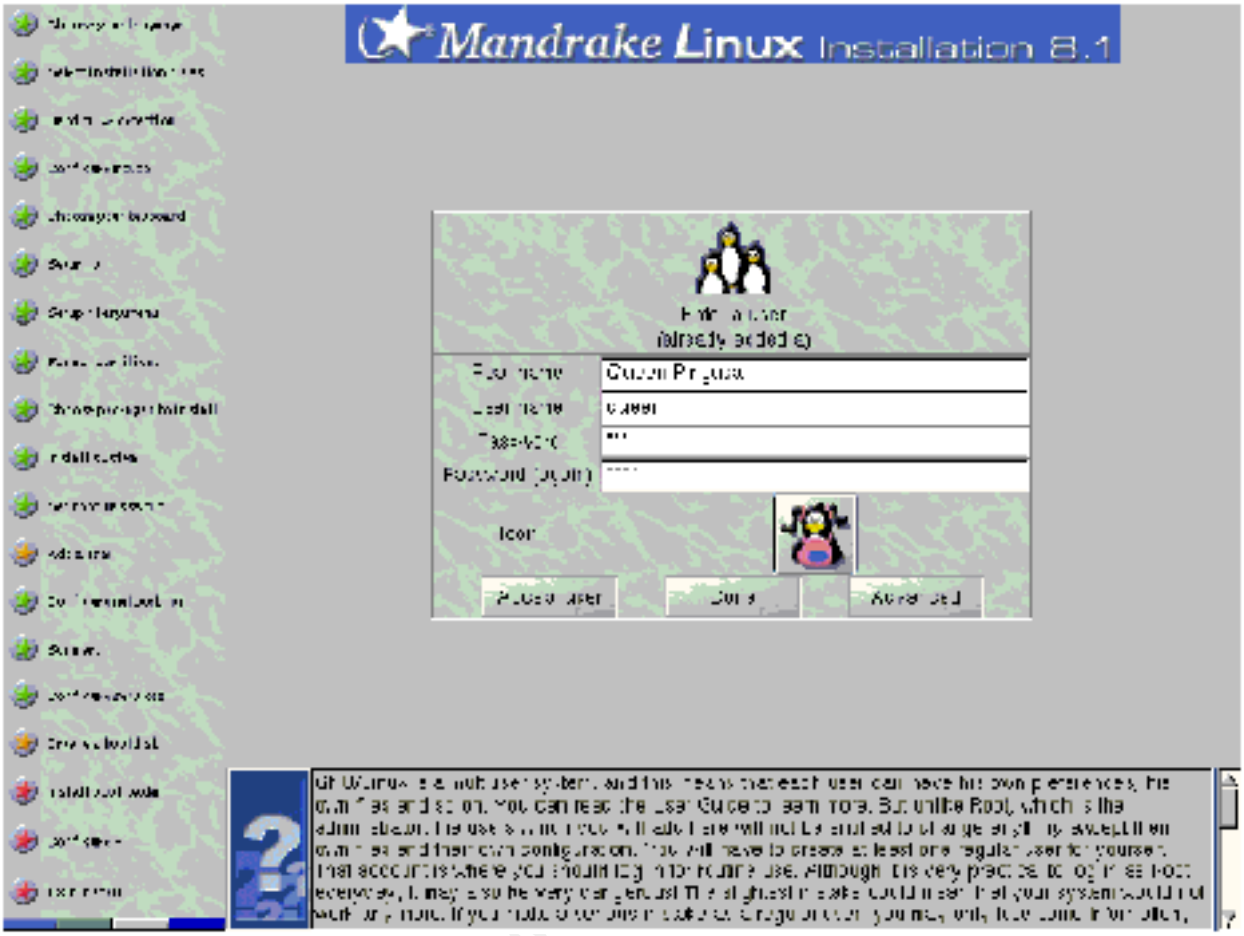
1.9 Root Password and Other Users

When the installation has completed, you are prompted for the "root" password. This is the most powerful password on the system. The owner of the root password can do anything he / she wants with the system because root is subject to no limitations.

Therefore, it is important that a good password is selected for root. A good password should be at least eight (8) characters long and contain a mixture of alphanumeric characters. Yet, the password should be easy for you to remember so that you do not have to write it down. For authentication use, the “Local files” or the option that best describes your network’s setup. My network uses neither NIS, nor LDAP for authentication. If you do have a network authentication server such as NIS or LDAP, it may still be preferable to authenticate locally to keep people from being able to log in remotely. Following the root password entry screen is the “Add a User” screen. Add a name for yourself here. This entry will later be used to test the security and access configuration. This new username should also be the one you use to login to the system on a regular basis. Given the limited control you have under this username you are less likely to cause accidental harm to the system. As root, however, you are much more likely to do something or make a mistake that could compromise the security of the system and its data. The screenshots below shows both the “root password” panel and the “Add a User” panel.



(Image from Mandrake Linux User’s Guide)



(Image from Mandrake Linux User's Guide)

1.10 Configure Networking

(Note: This option is not available in the Recommended installation option.)
Next, you are prompted to configure your network connection. The information in this section is based on your network configuration and address space. Linux will detect your network interface card (NIC) for you and then ask you to verify that it located the correct card and installation information.

1.11 Check Miscellaneous Parameters

Linux will then display a list of all the miscellaneous parameter information – mouse, keyboard, time zone, and printers. If the information it displays is correct simply click "OK", else click on the incorrect item and make the necessary changes.

1.12 Configure Boot Time Services

(Note: This option is not available in the Recommended installation option.)
This screen allows you to select what services you want to have started at boot time. If you are unsure about what a service is, simply click on the space between the service title and its corresponding check box. Since you know this is a web server, services such as the ones listed below should be the minimum services started at boot time:

- httpd – this service runs the Apache Web Server.
- iptables – the service automates a packet filtering firewall and will be used as a host-based firewall for this machine.
- preclude – this is a network intrusion detection tool.
- mysql – this is a database server. If you are extracting information from a database to provide dynamic content, it needs to be started with the web server.
- xinetd – provides access control, logging, and can place limits on the numbers of servers that can be started.
- network – this service activates and deactivates network interfaces, located in this machine, that are configured to start at boot time.
- syslog – this service is used to log messages from other daemons.

Your list of services may be longer than what is listed above, however, these services are definitely necessary at boot time for the system to perform its duties as a web server. Some of the risky services that you may not want to start at boot time are:

- portmap – this service manages RPC (remote procedure call) connections. RPC binds to a random port assigned by the kernel on startup. RPC then registers its port number with the portmap service which always listens on TCP (transmission control protocol) port 111 or UDP (user datagram protocol) port 111. Client machines that want to communicate with the RPC server need to find out what port the RPC server is listening on, so they query the portmap service. While turning off the service at boot time will not eradicate the problem, it may slow a potential intruder attempting to gain information on the services your machine is running. To really address this vulnerability you want to block spoofed IP (Internet Protocol) addresses, block access to port 111 (TCP and UDP), and block access to your ephemeral ports (port above 1023).
- netfs – is a file sharing service. It is always wise to disable file sharing with servers connected to the Internet. File sharing could give away network and system information to intruders, or make it easy for an intruder to gain unauthorized access to the system over the Internet.

Just remember to be very careful with the services you select to start at boot time. You will want to remove the services you do not need, but more importantly, you will want to remove the services that will create vulnerabilities.

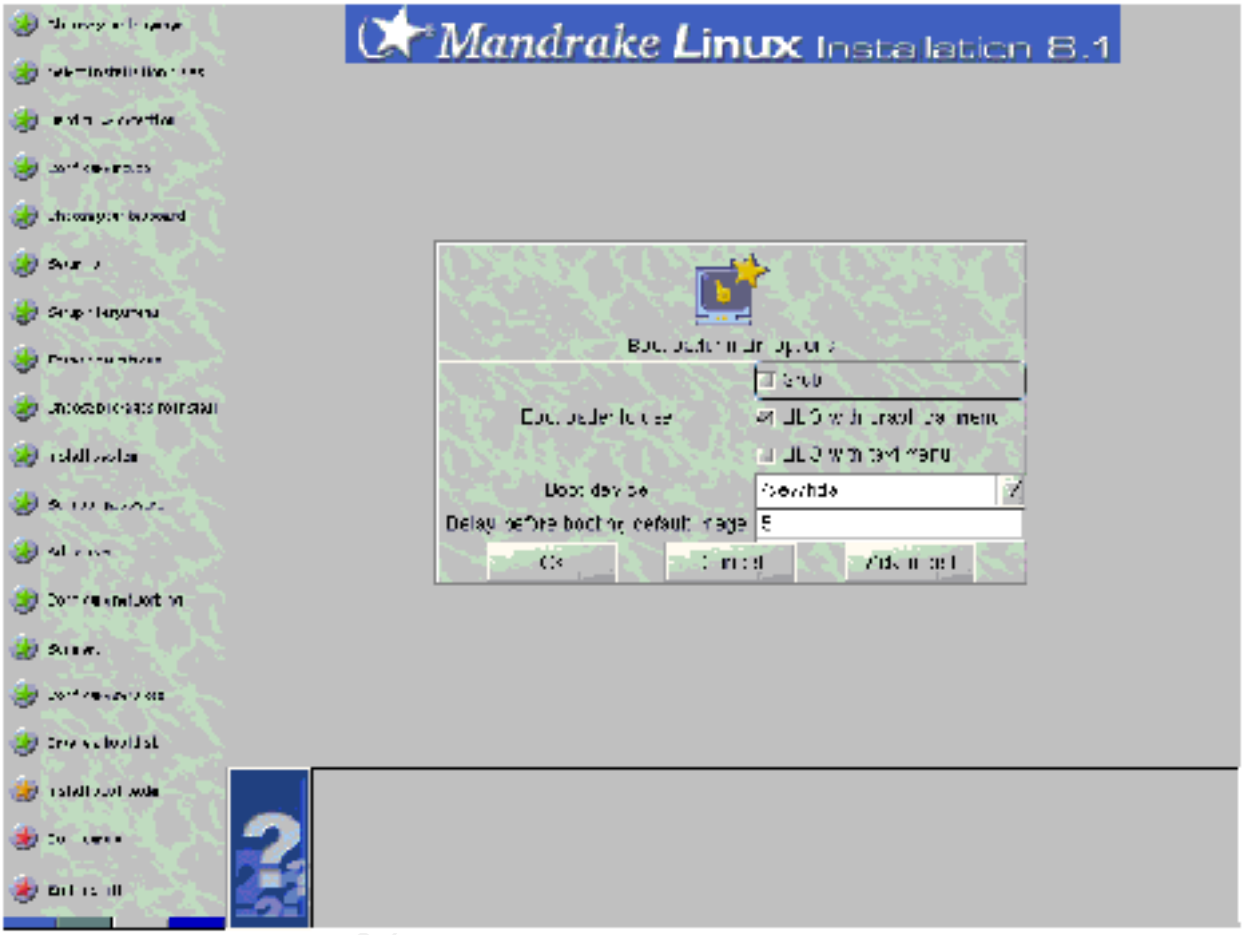
1.13 Boot Disk

(Note: This option is not available in the Recommended installation option.)
Now you have the opportunity to create a boot disk.

1.14 Installing Boot Loader

(Note: This option is not available in the Recommended installation option.)
From this screen, select the option that best describes your situation. Use GRUB if you have another OS on your machine and want to have a dual booting system.
Alternatively, load the LILO text or graphical menus. I selected the “LILO with graphical

menu" for my installation. While the screenshot below does not show this option, you can enter a password for the LILO boot loader. Taking advantage of the password option will prevent inexperienced people from rebooting the machine, and it will keep the machine from rebooting by itself. Since I prefer user involvement as opposed to automatic processes, I recommend entering a boot password for LILO.



(Image from Mandrake Linux User's Guide)

The boot loader screen also provides some advanced options that you may find beneficial. In particular, I elected to clear my /tmp files at each boot. This will prevent users or intruders from being able to retrieve information from temp files created as a result of any privileged actions that I may have taken while logged on to the system. You may also want to select the "Restrict command-line options" option. This is also not shown on the above menu.

During the boot loader installation, you will be asked if there are any additional operating systems installed on your hard disk. If no, accept the default settings by clicking on the "Done" button. If yes, click on the "Add" button and follow the instructions for adding the necessary parameters for the undetected OS. If you do not want anyone to have access to the other OS options shown by default, simply delete the parameter information for those OS installations. By deleting the OS parameters for

the other default entries, the only way to access those other OS options is by using a boot disk. For my installation, I have opted to remove the “failsafe”, and “Linux-2.2” OS parameters. This will help to slightly improve the security of the machine by requiring a boot disk, and minimizing the ways by which someone can log on to my machine.

1.15 Configure X, Graphical Server

(Note: This option is not available in the Recommended installation option.)
After finishing the boot loader installation you will be taken to the X Windows configuration screen. From this screen you will have the option to set up your monitor’s resolution. The setting is straightforward and Mandrake gives you a list of resolution options based on your video card. Simply select the setting that you desire and click the “OK” button. Next, you will be asked if you want the graphical server to startup at boot time. I answered yes to this question, because of my appreciation for the graphical user interface.

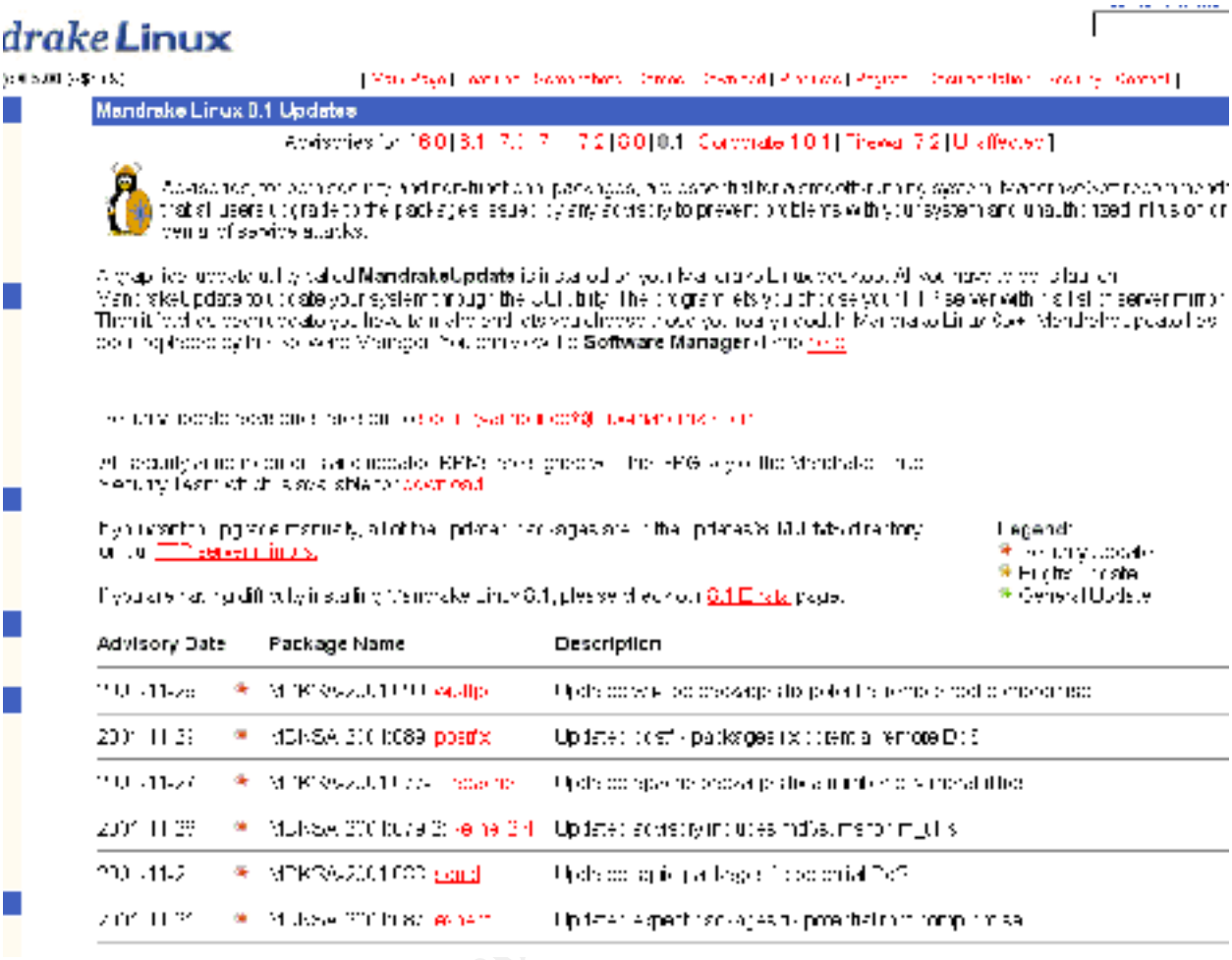
1.16 Exit Installation

When you get to the “Exit Installation” screen be sure to click on the “Advanced” button. This button gives you access to different floppy options. One floppy option allows you to create an installation disk, and the other option allows you to save your package selection to disk. I advise doing both of them before clicking “OK” to reboot your computer.

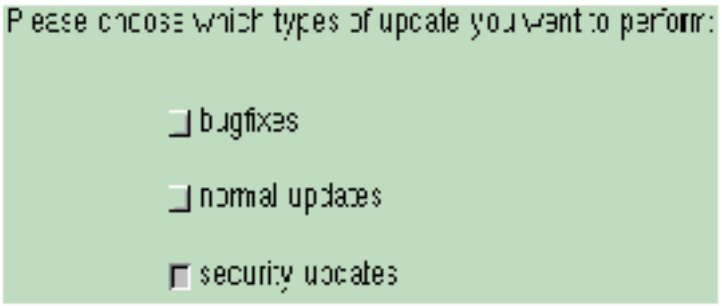
2. Securing the Operating System

2.1 Get Mandrake Linux Updates

Now that you have finally installed the operating system along with all the necessary packages, utilities, and modules, it is time to secure it. The first step in securing any system is to make sure that all the latest patches and hot fixes have been installed. You can find all the hot fixes, patches, and errata for Mandrake at http://www.linux-mandrake.com/en/, and clicking on the security link on the top of the page. The next page shows an image of the Mandrake Linux Update page.



All Mandrake updates can be done automatically using the “MandrakeUpdate” wizard. Simply click on the “MandrakeUpdate” button in the “RpmDrake” tool bar to launch the wizard. A panel will then pop up asking for the type of update you would like to perform. Your update choices are “bug fixes”, “normal updates”, and “security updates”. I recommend doing all updates, however if you are pressed for time, the “security updates are a must. The picture below is a screenshot of the update wizard interface.



(Image from Mandrake Linux User’s Guide)

Here is a general definition of each of the update types:

- Bug fixes – this type of update will repair problems with software that does not operate, as it should. Generally, these types of problems are a nuisance and do not create any security threat.
- Normal updates – this type of update is similar to a software upgrade. It may add new features to an existing application to improve it functionality.
- Security updates – these are the most important updates because they may help to solve a potential vulnerability in your software. If these are not updated regularly, your system is more likely to be compromised by hackers.

2.2 Building a Custom Kernel

Building a custom kernel for your server is a good idea if you want to optimize the performance of the Linux kernel for your specific hardware. It is also a good idea to customize your kernel if you want to have a new feature compiled in with your kernel or if the new kernel has additional features, that would benefit your system. The primary reason for customizing the kernel here is to make sure that this system is running the latest kernel and to eliminate drivers and services that you do not want or need. The following information can be used to help you configure your kernel.

1. *Download the latest kernel, e.g. linux-2.4.16.tar.gz.*
2. *rm /usr/src/linux*
3. *cd /usr/src; tar xvfz /some/path/linux-2.4.16.tar.gz*
4. *ln -s linux-2.4.16 linux*
5. *cd /usr/src/linux*
6. *make menuconfig (or make xconfig if using X Windows)*

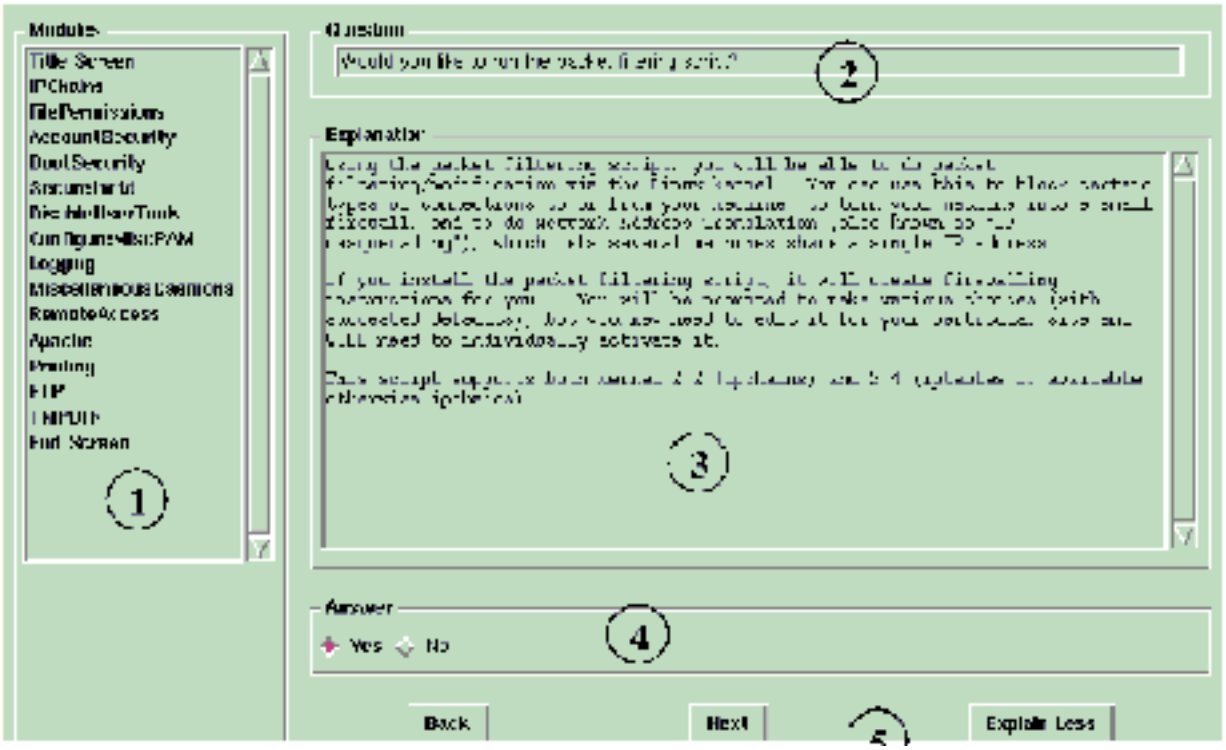
At this point, a menu will appear that presents you with all the possible hardware and software configurations. Answer 'N' to all hardware not on your system. Answer 'N' to all software unnecessary for your web server, e.g. amateur radio, telephony, ISDN, etc. When you have made all or your selections and you are at the end of the menu, click Exit (Menuconfig). This will create a file called "*.config*'" containing all the configuration options you selected during the process. Once your configuration file matches your hardware and desired software, build the new kernel and put it into place by:

7. *cd /usr/src/linux*
8. *make dep*
9. *make bzImage*
10. *make modules*
11. *make modules_install*
12. *cp System.map /boot/System.map-2.4.16*
13. *cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.16*
14. Edit the file */etc/lilo.conf* to include the new kernel you just built.
15. Run */sbin/lilo* to re-install the boot loader with the new kernel information.
16. Re-boot your system to see if the new kernel will run.

If you require additional assistance with this process study the document on how to build a Linux kernel, which can be found at: Kernel-HOWTO http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html.

2.3 Configure Bastille

Mandrake Linux comes with Bastille security tools suite. The tool suite has two types of configurations, a basic configuration, and a complex configuration. The basic configuration tool called the BastilleChooser is for the novice user. The advanced and more complex configuration is called the InteractiveBastille. This application is suited more for the experienced user. To launch, type InteractiveBastille at the command prompt. This tool has wizards for various services, such as the Apache Web server, IP Chains, account security, boot security, etc. Going through some of these wizards will help you to set up your system to your desired security level. My recommendations for securing a web server with the aforementioned specifications is to do the Apache, remote access, boot security, logging, configure MiscPAM, account security, and miscellaneous daemon wizards. Running these wizards will cover many other concerns with this server. I did not select FTP or IP Chains because no FTP services have been installed and because the next security feature will address firewalls. A screenshot of the InteractiveBastille panel is below.



(Image from Mandrake Linux User's Guide)

The numbers on the picture correspond to the descriptions below:

1. This menu displays the many available security configuration wizards.

2. This field shows the current question asked by the wizard. Your answers help to define the level of security.
3. This frame provides background information with regard to the question being asked.
4. Submit your answers in this field by selecting “Yes” or “No” or providing input.
5. Navigation buttons.

2.4 Setting Security Level – The Control Center

Under the “Security” icon of the control center is a “Security Level” option that will allow you to set the security level of your machine. This panel provides a graphical user interface for the “MSEC” security application for Mandrake Linux. MSEC is designed to operate on highly visible systems that are constantly connected to the Internet, such as a public web server. MSEC consists of two parts:

1. Scripts that define the various security levels from 0 to 5, with level 0 being the lowest level of security and level 5 being the highest.
2. Cron jobs that will periodically check the system according to the selected security level, to detect and warn you of possible intrusions, security leaks, and vulnerabilities.

MSEC is also flexible enough to allow the user to customize his or her own security setting. However, from the graphical interface you have only three levels to choose from, “Low”, “Medium”, and “High”. During the “Expert” installation mode described earlier, you selected the “High” security level, however, you were not able to select “libsafe” option. The “libsafe” option is necessary for machines that are continuously connected to the Internet, or acting as an Internet server. “Libsafe” is a library that can prevent attacks that can cause buffer overflows, and is therefore a highly recommended setting. Therefore, from this panel, you can select this option, and from the MSEC application, you can customize your own security level. I set up a custom MSEC security level by typing

```
msec custom
```

This will start the script program and allow you to make whatever changes you want. I ended up only making a change to the level 4 setting, which allowed all computers to connect to all open ports. I felt this was adequate because the only ports I plan to have open for this web server are 80 and 443. If you simply want to select one of the default settings, type

```
msec <x>,
```

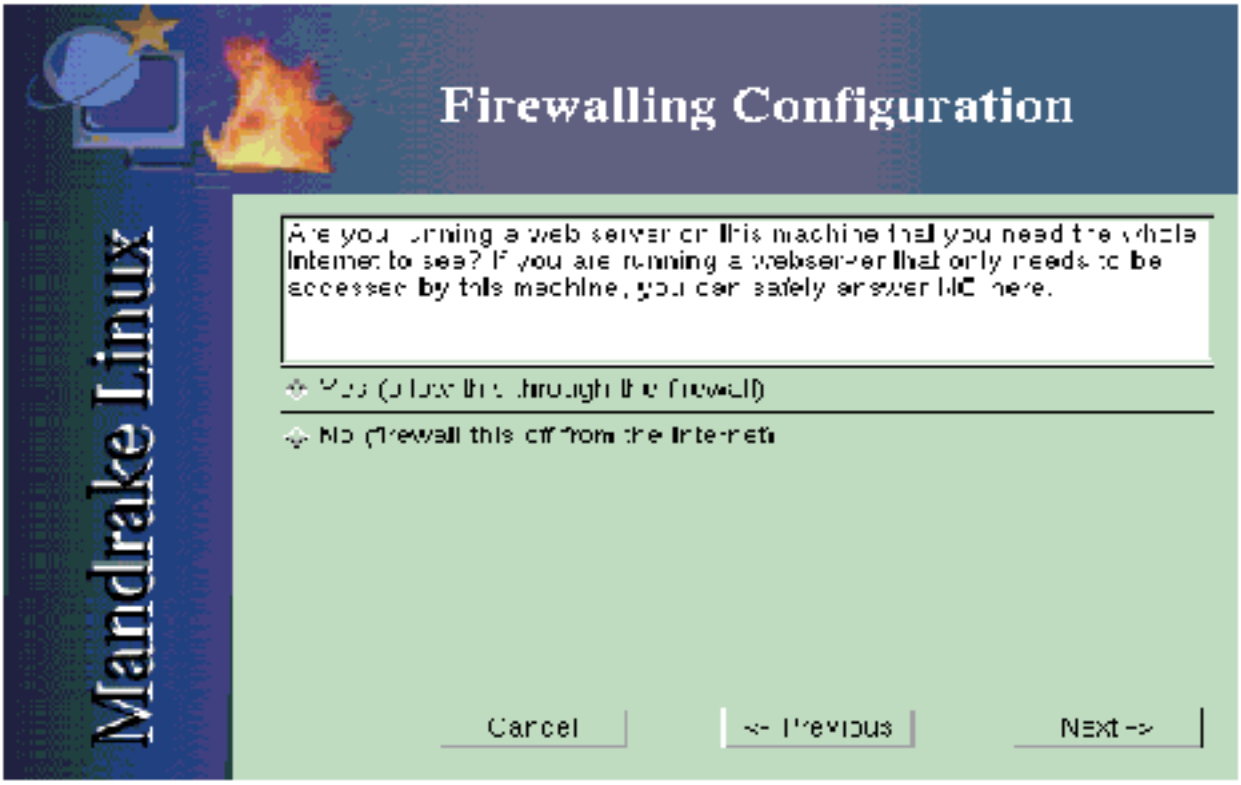
where <x> is any number 0 through 5. The next page shows a screenshot of the security features available through the MSEC security application.

Feature \ Level	0	1	2	3	4	5
global security check			yes	yes	yes	yes
umask for users	002	002	002	002	077	077
umask for root	002	002	002	002	002	077
Feature \ Level	0	1	2	3	4	5
shell without password	yes					
authorized to connect to X display	all	local	local	none	none	none
user in audio group	yes	yes	yes			
. in $PATH	yes	yes				
warnings in file /var/log/security.log		yes	yes	yes	yes	yes
warnings directly on tty			yes	yes	yes	yes
warnings in syslog			yes	yes	yes	yes
warnings sent by e-mail to root			yes	yes	yes	yes
suid root files check			yes	yes	yes	yes
suid root files MD5 check			yes	yes	yes	yes
writable files check				yes	yes	yes
permissions check				yes	yes	yes
suid group files check				yes	yes	yes
unowned files check				yes	yes	yes
promiscuous check				yes	yes	yes
listening port check				yes	yes	yes
passwd file integrity check				yes	yes	yes
shadow file integrity check				yes	yes	yes
system security check every day at midnight				yes	yes	yes
all system events additionally logged to /dev/tty12				yes	yes	yes
Only root can ctrl-alt-del					yes	yes
unknown services are disabled					yes	yes
boot password (grub/LILO)					yes	yes
grants connection from	all	all	all	all	local	none

(Image from Mandrake Linux User's Guide)

2.5 Firewall Configuration – The Control Center

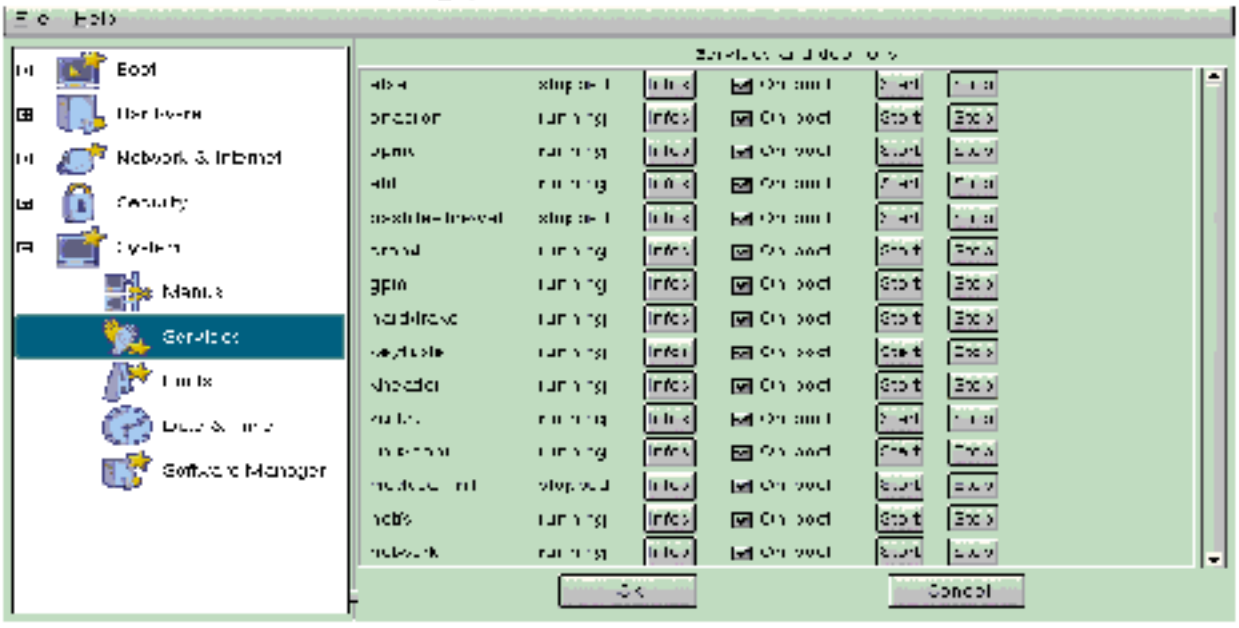
The next image is of the "Firewall Configuration" panel. This panel is part of a wizard that will take you through the steps of configuring a network or host-based firewall for your system. Since this system is, setup to be a web server, and not a router, the purpose of running this wizard is to set up a host-based firewall. Once you start the wizard all you have to do, is answer the questions based on your network set up? Once you have completed the wizard you are asked if you would like to activate the firewall. Simply, click the "Save and Quit" button and then the "Finish" button to restart the firewall with your new rule. The goal of configuring this firewall is to permit connections to TCP ports 80 (HTTP) and 443 (HTTPS) only.



(Image from Mandrake Linux User's Guide)

2.6 Check Startup Services – The Control Center

Mandrake provides a great interface for viewing the files that run automatically when the system boots. This panel is very helpful if you would like to know what services are starting at boot or any additional information about a particular service.



(Image from Mandrake Linux User's Guide)

If you want to change the startup setting of a service simply, click on the check box that corresponds to that service. Likewise, if you need to stop or start a service click on the appropriate start or stop button for that service. The screenshot on the bottom half of the previous page is only meant to show what the panel looks like. It is not intended to be used as a guide for what services are to be set for this web server.

2.7 Disable Rebooting with Ctrl+Alt+Del (may not be necessary if using MSEC level 4 or 5)

This step will keep people from unintentionally, or intentionally rebooting your server. This can be done by simply commenting out the "ca" option as seen below:

```
#ca::ctrlaltdel:/sbin/shutdown –t3 –r now
```

2.8 Require Root Password for Single User Mode

Since single user mode is equivalent to root access. Some Linux OS's do not require a password for single user mode. Check to make sure yours does. If it does not, simply add this line after the "si" option:

```
~~:S:wait:/sbin/sulogin
```

2.9 Turn off inetd

It is a good idea to disallow services in /etc/inetd.conf. If you have set up your computer this way you can simply turn off inetd. If you decide to do this, use the statements below to turn off inetd.

```
[root]# /etc/rc.d/init.d/inet stop
[root]# /sbin/chkconfig inet off
```

2.10 Check for .rhosts files in Home Directories

Due to the security problems that surround the "rsh" and "rlogin" programs you should check to ensure that none of the user accounts have a .rhosts or a /etc/hosts.equiv file in their home directory. The reason for concern stems from the fact that these files are used by the "rsh' and "rlogin" programs to assign "trust" privileges to users on other computers. To check for the aforementioned files you can run the script below.

```
#!/bin/sh
for I in `cut –d: -f6 /etc/passwd`; do
        if [ -e $i/.rhosts ]; then
                echo "Security check found .rhosts in $i"
        fi
done
```

2.11 Prevent Cores

Core files are created when a system process aborts unexpectedly. They typically contain debugging information that is valuable for troubleshooting the cause of the unexpected process termination. Core files usually contain a complete image of the

memory allocated to the process at the time of the crash. Using the strings program any one can read the information in a core image file, because core files are world-readable. Subsequently, if a process that reads passwords out of /etc/passwords or /etc/shadow crashes in this manner and a core file is remaining, the information in those /etc files can be read by any one, using the strings program. You can prevent this from occurring by typing the command below:

limit coredumpsize 0 # csh,

into the /etc/profile or /etc/.login files.

2.12 Set Password Expiration (may not be necessary if using the Bastille Account Security wizard.)
Passwords must be managed appropriately in order to be effective. Keeping a password active too long will compromise the security of your information system. The longer an intruder has to attempt to crack your passwords the more likely the intruder is to succeed. To prevent this from occurring you should enforce password expiration to force users of your machine to change their password on a regular basis. The command below can be used to set password expiration and reminders.

[root]# chage –M 120 –W 10 <username>

The above statement says that the person who goes by <username> must change their password every 120 days and will be reminded of the impending change 10 days before the password expires.

2.13 Run the SANS "newperms" script
The "newperms" script, provided by SANS, changes the default permissions on your Linux files to reduce the leaking of unnecessary and potentially dangerous information to the user. This program will prevent users from performing actions that could pose security risks to the files on your system. You should download and run this script whenever you add updates to your system or reinstall linux. Simply, download the script from SANS at http://www.sans.org/linux.htm and run the script as shown below. You will probably receive a few errors because some of the packages that the script is looking for may not have been installed due to the customized installation.

[/root]# sh newperms

2.14 Locate Active Services (A Configuration Test)
Perform this procedure last to test your system and server configuration. By using the "netstat" application, you are able to view all active and listening services. This is beneficial because it will tell you if have any services running that you do not want to run. Simply type the command below to see all of the active TCP connections and corresponding ports.

[root]# netstat –atp

If you have successfully applied the system security features discussed in this tutorial, you should get a read out similar to this:

```
Active Internet connections (servers and established)
Proto  Recv-Q      Send-Q      Local Address          Foreign Address      State
       PID/Program name
tcp    0           0           *:netbios-ssn          *:*                  LISTEN      724/smbd
tcp    0           0           *:www                  *:*                  LISTEN      683/httpd
```

Netstat can also be used to test the server's vulnerability to certain packets and connection requests. You can do this by running the display in one second intervals while remotely trying to connect to a service that you have deactivated or is listening. You can then monitor the changes in the state of the service, port, and protocol it uses.

3. Securing the Web Server

3.1 Set Default Deny Access

When setting up rules for highly accessible systems such as Internet servers, it is a good idea to set permissions to a default deny, such that if things go wrong the system will fail in a closed state. Below is the default deny script for the Apache web service.

```
<Directory />
Options None
AllowOverride None
order allow,deny
deny from all
</Directory>
```

These instructions are located in the access.conf file. It denies access to all directories and files. You should also put loop back and non-routable IP addresses in the deny instructions to prevent spoofing.

3.2 Set Specific Access

This access information also goes into the access.conf file. These rules permit access to the specific areas of your file system. The information used in the previous and following access instruction is sample information. You will have to fill in the information according to your file system set up and IP address permissions

```
<Directory /http/docs>
AllowOverride AuthConfig
order allow,deny
allow from 192.168.
deny from all
</Directory>
```

3.3 Add "index.html" to All Web Directories

Adding "index.html" to all your web directories will prevent casual users from viewing files that are meant to be hidden or files to which otherwise they would not be able to access. Without the "index.html" file all of the contents of the directory entered in the URL, are listed in the browser window. With the "index.html" you could just leave the file blank, or put a message telling the user to go back, or write JavaScript program that will take the user back to the home page. Regardless of what you do with the file just be sure to have it in each one of your web directories.

However, if you want to use the HTTP protocol to distribute files this may be a much easier and safer solution than using FTP, if configured correctly.

A huge security leak could occur if you were using ".htaccess" files to enforce permissions and some one was able to get a directory listing. When a browser lists the contents of a directory the information in that directory is downloadable, hence your ".htaccess" file could then be downloaded by anyone.

3.4 Prevent ".htaccess" Requests

If you are using ".htaccess" a clever hacker may try to access your ".htaccess" file through the URL. Using the following file directive can prevent this.

```
<Files ~ "^\.ht">
order allow,deny
deny from all
</Files>
```

The directive will deny access to any file that begins with the three characters ".ht".

3.5 Password Protection

The directive below is used to protect passwords in the specified directory. This directive says that the users that have access to "/usr/local/apache/htdocs/private" are found in the "/usr/local/apache/conf/members" directory.

```
<Directory /usr/local/apache/htdocs/private>
AuthName "Private Parts"
AuthType Basic
AuthUserFile /usr/local/apache/conf/members
require valid-user
order deny,allow
allow from all
</Directory>
```

3.6 Limit CGI's Access

Use the <File> directive below to prevent unwanted CGI access:

```
<Files ~ "*(\~|\.cgi.+)$”>
Order deny,allow
Deny from all
</Files>
```

3.7 Install SSL

Use SSL to encrypt connections between the user and the web server. SSL will keep passwords and usernames from being sent in the clear and prevent a man-in-the-middle attack. You must have OpenSSL installed on your machine. To create a private key using the triple DES encryption standard use the command below:

```
openssl genrsa -des3 -out filename.key 1024
```

Your private key will be created in the current directory. Next, you will have to create a certificate-signing request (CSR). This can be accomplished by locating the private key that you would like to generate the CSR from and typing in the following command:

```
openssl req -new -key filename.key -out filename.csr
```

You will then be prompted for information such as your domain name. Send this CSR to a certificate authority such as Verisign and follow their instructions. Once you have received your signed certificate from the certificate authority, place it in the designated directory. Now you must set up a secure virtual host. An example of a secure virtual host can be seen below.

```
<VirtualHost 172.18.116.42:443>
DocumentRoot /etc/httpd/htdocs
ServerName www.somewhere.com
ServerAdmin someone@somewhere.com
ErrorLog /etc/httpd/logs/error_log
TransferLog /etc/httpd/logs/access_log
SSLEngine on
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
SSLCACertificateFile /etc/httpd/conf/ssl.crt/ca-bundle.crt
<Files ~ "\.(cgi|shtml)$">
SSLOptions +StdEnvVars
</Files>
<Directory "/etc/httpd/cgi-bin">
SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
CustomLog /etc/httpd/logs/ssl_request_log \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

Next, using ModSSL turn on SSL by typing the command, “SSLEngine on”. Now you should restart the server with the following commands,

```
httpd stop
httpd startssl
httpd restart
```

or

```
apachectl stop
apachectl startssl
apachectl restart
```

Your web server should now be SSL enabled.

3.8 **Check the Configuration** (A Configuration Test)

Now that you have completed the setup of Apache, it is a good idea to test your setttings. In particular, test your new SSL with PKI certificate to make sure that it works properly by typing your domain name preceded by “https://” in the address bar. It should look something like this,

https://computerName.company.com

You may get a pop up message telling you that you are about to connect to a secure server or environment. The next item you may want to check is the “.htaccess” prevention setting. Simply enter a URL that goes directly to a “.htaccess” file. See below:

http://computerName.company.com/docs/.htaccess

This should return a “403 Forbidden” error message or something. Ultimately you want to test all the configuration settings to ensure that they are all working properly and to make sure that you configured them correctly. It may take a while, but a little time now will save a lot of time later.

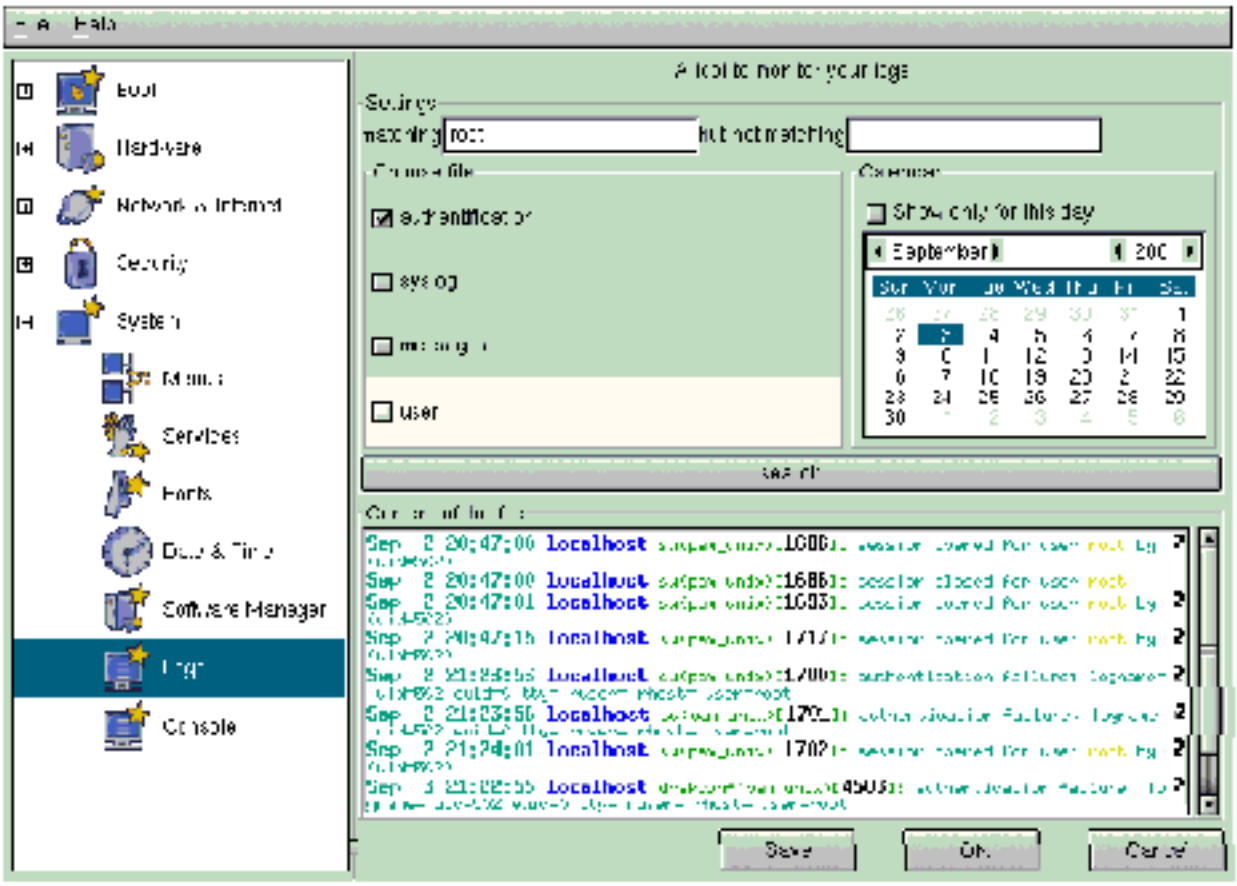
4. System Administration

Administering the server now that it has been completely set up is an ongoing process. System administration takes into consideration keeping up with the latest patches, upgrading software, hardware, and troubleshooting among other responsibilities. However, while recognizing that the term system administration sums up a number of duties, for the purposes of this section of the tutorial, system administration will only refer to log file analysis and backups.

4.1 Log File Analysis

All system administrators are responsible for examining log files. Applying the MSEC system security application makes log analyses much easier, because all warnings

and/or alerts are sent to the syslog. What really makes it useful is the fact that MSEC incorporates its own small file integrity analyzer (FIA), which also logs information into the syslog if it finds something suspicious. The FIA that comes with MSEC monitors changes in the MD5 signature for each of the suid root files on the system. If a change is found a warning is issued. This warning, of course, goes to the syslog. However, MSEC can also be set up to issue warnings to the root via e-mail. Along, with doing MD5 signature checks on suid files, MSEC checks for file permissions, unknown files, world writable files on the system, as well as some other checks. If anything it examines appears to be insecure or suspicious it will send a warning to the syslog. Therefore, the system administrator simply has to keep up with the logs and investigate suspicious entries. The syslog for Mandrake has a very useful interface as seen below.



(Image from Mandrake Linux User's Guide)

This panel allows you to sort by word, day, and log in a very bright easy to read graphical user interface. These sorting features make it easy for you to search for particular incidents and security threats.

4.2 Backup the Server

The final task for completing this tutorial is the backup of the system. A large amount of time has been spent testing the configuration and getting it just the way you want. That being said, now is a good time to save all the data on your hard disk to the removable

Iomega 20 GB disk. The fact that the disk is removable is beneficial because now the backup disk can be taken off site and locked up for safekeeping. You should have several of these disks so that you can develop a backup schedule for rotating which removable disk to back up to. Nevertheless, for now we will deal with the one disk. To run the back up type the following commands at the console:

[/root]# init 1 (puts the system into single user mode)
[/root]# dd if=/dev/hda of=/dev/hdb (where /dev/hdb is the designation for the external disk)

Use the following command for all partitions except for any extended partitions or swap:

[/root]# fsck –y /dev/hdb# (where # is the partition number on the external disk).
[/root]# init 3 (returns the system to multiuser mode)

Conclusion

To end this tutorial I would like to pick up where I left off at the beginning of the Server Administration section. In the first paragraph of that section I stated some of the responsibilities of a system administrator. Now that you have configured a secure web server, and are ready in put it in the middle of the Wild Wild West (WWW), the real work is just beginning. Mandrake has provided a number of tools to help you survive the harsh Internet environment, but you must take advantage of them. You must read your syslogs, constantly test your machine for vulnerabilities, pay close attention to available updates, and simply be smart. Hopefully, I have taught you well and you will be able to use this tutorial as a reference, in the future.

Good Luck!

Bibliography

Bastille Linux
URL: http://www.bastille-linux.org/ (November 26)

OpenSSL Documents, openssl(1)
URL: http://www.openssl.org/docs/apps/openssl.html (November 26)

OpenSSL Documents, ssl(3)
URL: http://www.openssl.org/docs/ssl/ssl.html (November 26)

WWW Security FAQ Running a Secure Server
URL: http://www.w3.org/Security/Faq/wwwsf3.html (November 26)

SANS Institute Resources. "Securing Linux Step-by-Step."
URL: - http://www.sans.org/linux.htm (08 November 2001).

NSWC Dahlgren. "SHADOW Version 1.7 Installation Manual."
URL: http://www.nswc.navy.mil/issec/ (08 October 2001).

Security Quick-Start HOWTO for Linux
URL:
http://www.linuxsecurity.com/resource_files/documentation/QUICKSTART/index.html
(13 November 2001).

secure_webserver.txt
URL: http://www.net-security.org/text/articles/dl/secure_webserver.txt (13 November 2001).

How to stop crackers with PortSentry - Oct 3, 2001
URL: http://www.linuxworld.com/site-stories/2001/1002.portsentry.html (November 26)

10 minutes to an iptables-based Linux firewall - Sep 20, 2001
URL: http://www.linuxworld.com/site-stories/2001/0920.ipchains.html (November 26)

Freeware Security Web Tools
URL: http://www.samag.com/print/documentID=16832 (November 20)

Linux Documentation. "SSL Red Hat How To" URL"
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/SSL-RedHat-HOWTO.pdf (15 November 2001).

Linux Documentation. “Firewall-HOWTO” URL”
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/Firewall-HOWTO.pdf
(15 November 2001).

MandrakeSoft. “Mandrake Linux 8.1 Reference Manual.”
URL: http://www.linux-mandrake.com/en/ (November 26)

MandrakeSoft. “Mandrake Linux 8.1 User’s Guide.”
URL: http://www.linux-mandrake.com/en/ (November 25)

Stephen Gibson. “Installing and Securing a Shell Access Server Using Red Hat 6.2 Linux.”
URL: http://www.sans.org/y2k/practical/Stephen_Gibson_GCUX.doc. (November 26)

David Koconis. “Step-By-Step Guide to Configuring an SSL Enabled Web Server that Access a Backend Database using RedHat 7.0”
URL: http://www.sans.org/y2k/practical/David_Koconis_GCUX.doc. (November 26)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**