Network Intrusion Detection

Best of Breed Protection with SNORT

Implementing Snort

Snort can be readily implemented with the help of a special Linux distribution named Sentinix (http://www.sentinix.org). Wait a minute, you ask, Linux? Isn't that complicated? All my systems are Microsoft!

The short answer – yes. Snort should indeed be implemented using Linux. The Sentinix distribution makes this an easy and painless process – much easier than configuring a Windows server and installing Snort. Snort sensors should be viewed as appliances (like a router or a UPS) and as such, do not need to integrate with your server infrastructure. In fact, you probably have other network appliances running on some version of Linux. One last consideration is if your intrusion detection system is on the same platform as the rest of your systems, it may become compromised along with your other systems in the event of a successful intrusion.

About Sentinix

Sentinix is a special-purpose distribution of Linux that contains a preconfigured environment for running Snort. In addition to Snort itself, Sentinix includes:

- SnortCenter management console
- ACID intrusion analysis and reporting system
- Supporting applications: Apache, PHP, Perl, Python, and MySQL
- E-mail tools: Postfix, MailScanner, SpamAssassin
- Other tools: Nessus, Nagios, Nagat, Cacti, RRDtool
- And more…

For small installations, a single computer can monitor the network and house the management applications (SnortCenter and ACID). In larger deployments, you will probably want to separate these functions. One computer can perform the management functions while other computers act as sensors. Figure 1 shows a typical arrangement of sensors within a medium sized network.

Sentinix is designed to provide a secure, lightweight environment and, therefore, runs only a minimal set of normal Linux services. Memory intensive services such as X-windows and other unnecessary services such as BIND (DNS server), DHCP server, etc., are not included with Sentinix.

For additional information, go to http://www.sentinix.org.

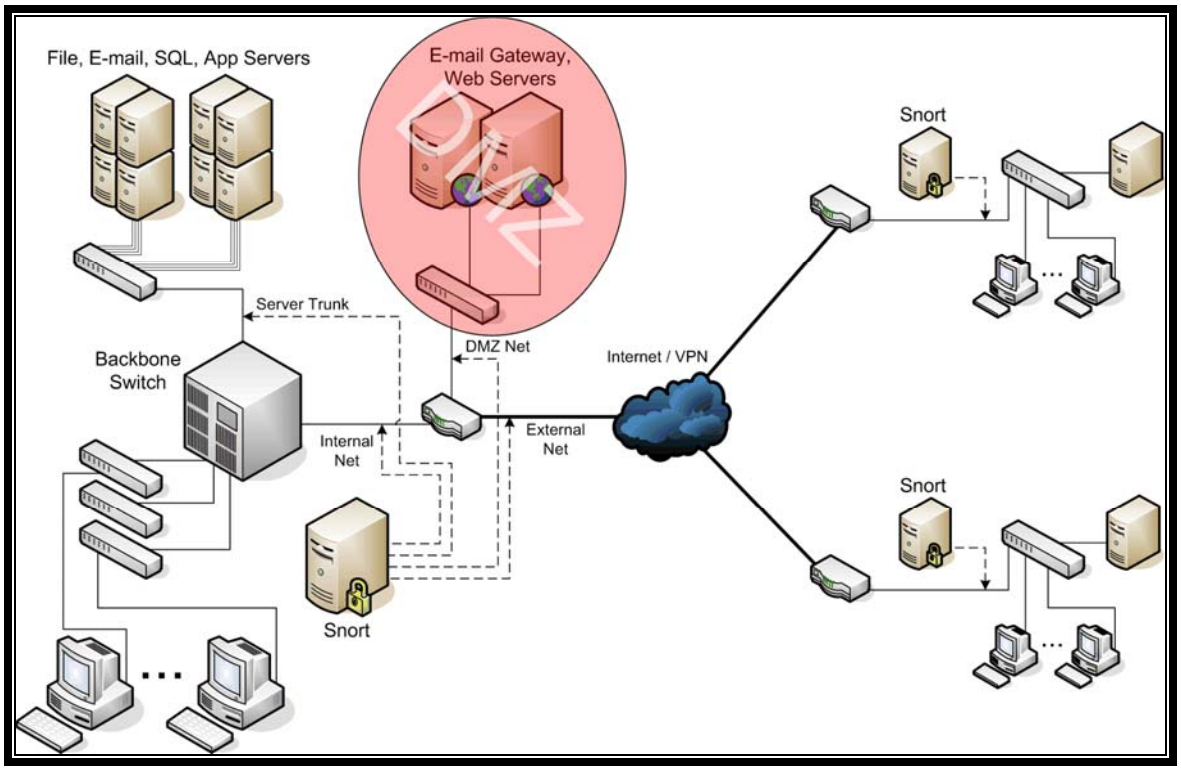


Figure 1 - Placement of Snort Sensors

Hardware Requirements

The hardware requirements for Sentinix are minimal. A sensor can easily run on a 1Ghz machine with 256MB RAM and a 4GB hard disk. As with any system, more is better. A machine that is housing the management applications will do better with 512MB RAM and a hard disk that can accommodate the amount of log data that you wish to keep online.

Downloading Sentinix

Sentinix is supplied as an ISO image that can be burned to a CD-ROM. The current version of Sentinix is 0.70.5 and can be downloaded from one of the mirrors listed at http://www.sentinix.org/downloads.shtml. The file you want to download is named *sentinix-0.70.5.iso*. Once the file has been downloaded, burn the image to a CD-ROM. Note that you *must* write the ISO image to a CD-ROM, not simply copy the ISO file to a CD-ROM. Most CD burning programs have a command called “Burn Image” or something similar that will accomplish this.

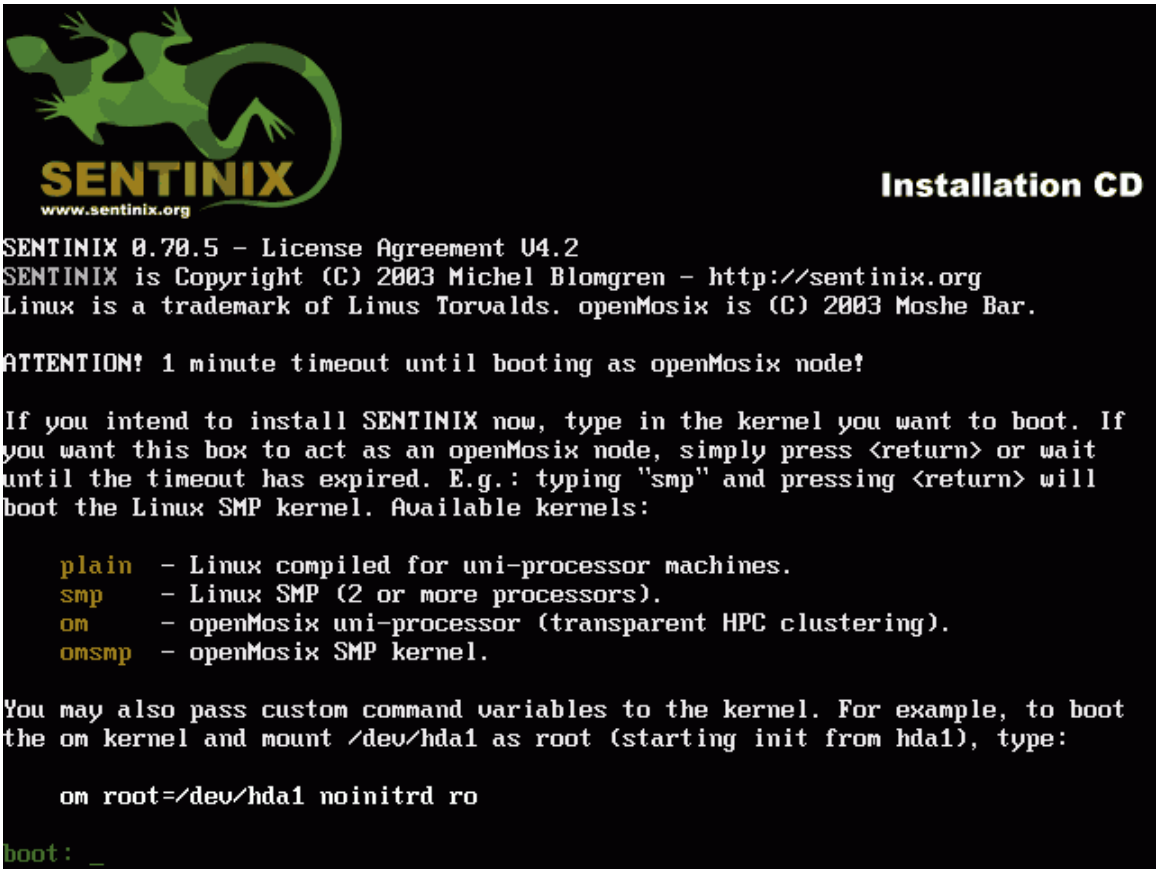
Installing Sentinix

Installing Sentinix is a straightforward process. Use the following steps and screenshots as a guideline. It is possible that the procedure will deviate slightly based on your unique situation.

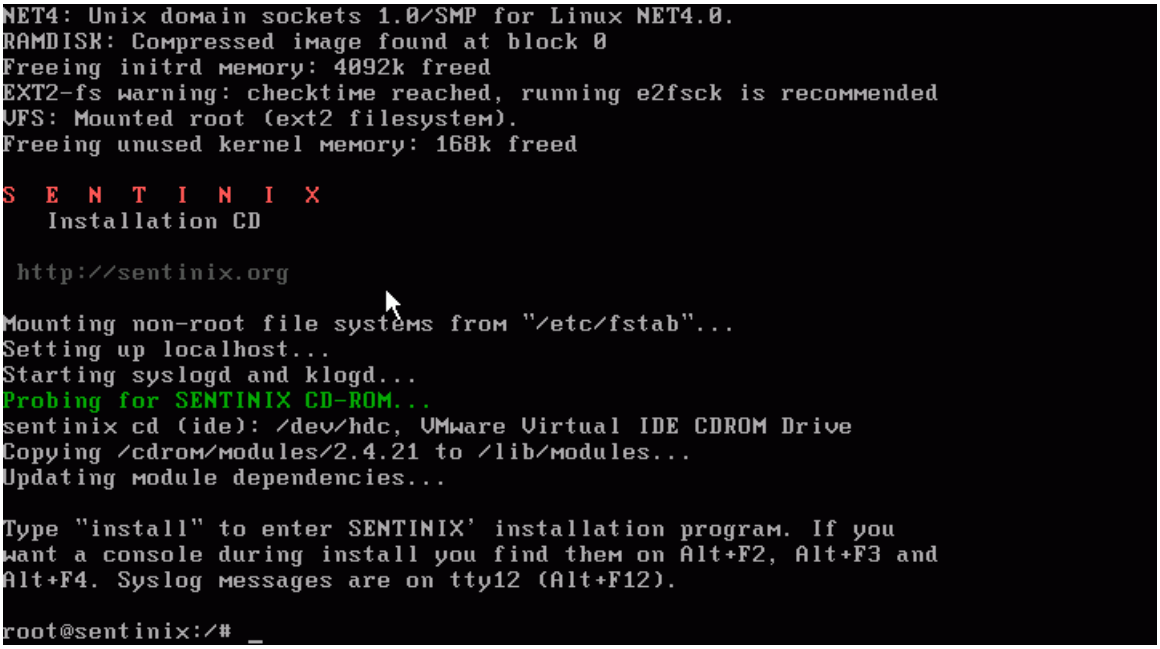
Note: These instructions are adapted from the Sentinix Installation Guide.

1. Prepare a host machine for Sentinix.
2. Go into the BIOS and set the clock to the current GMT time.

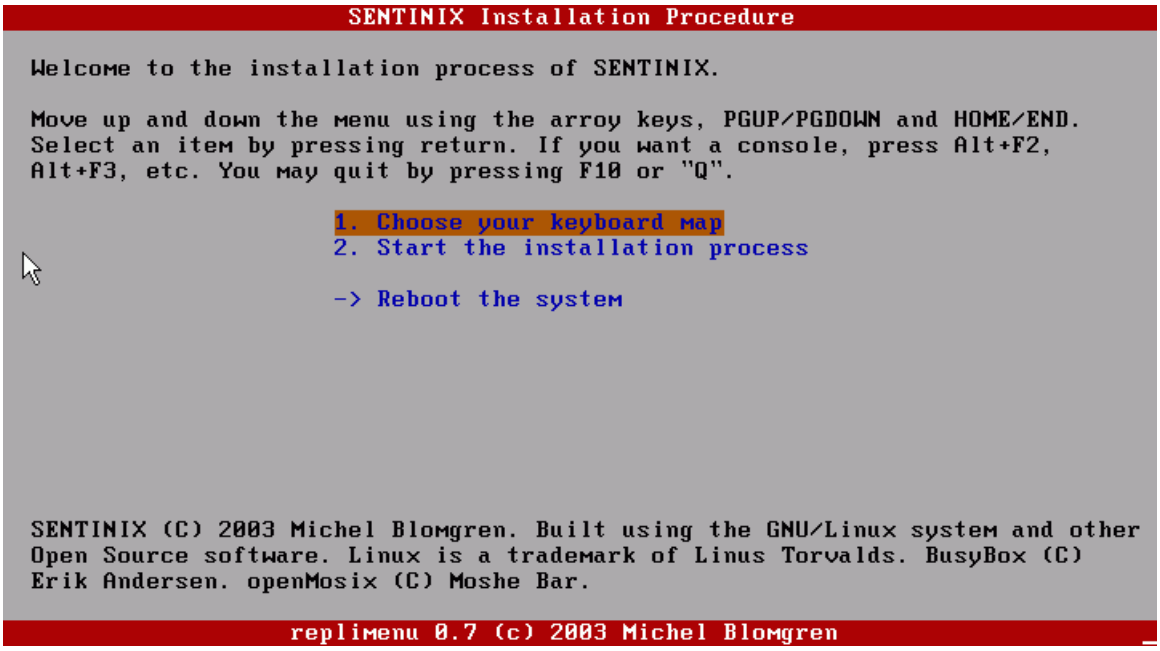
3. Insert the newly created SENTINIX CD in the CD-ROM drive and boot up. Make sure that the BIOS boots from the CD-ROM!



4. At the boot prompt, type “plain” and press Enter.



5. Once the system has booted from the CD-ROM, type “install” and press Enter.



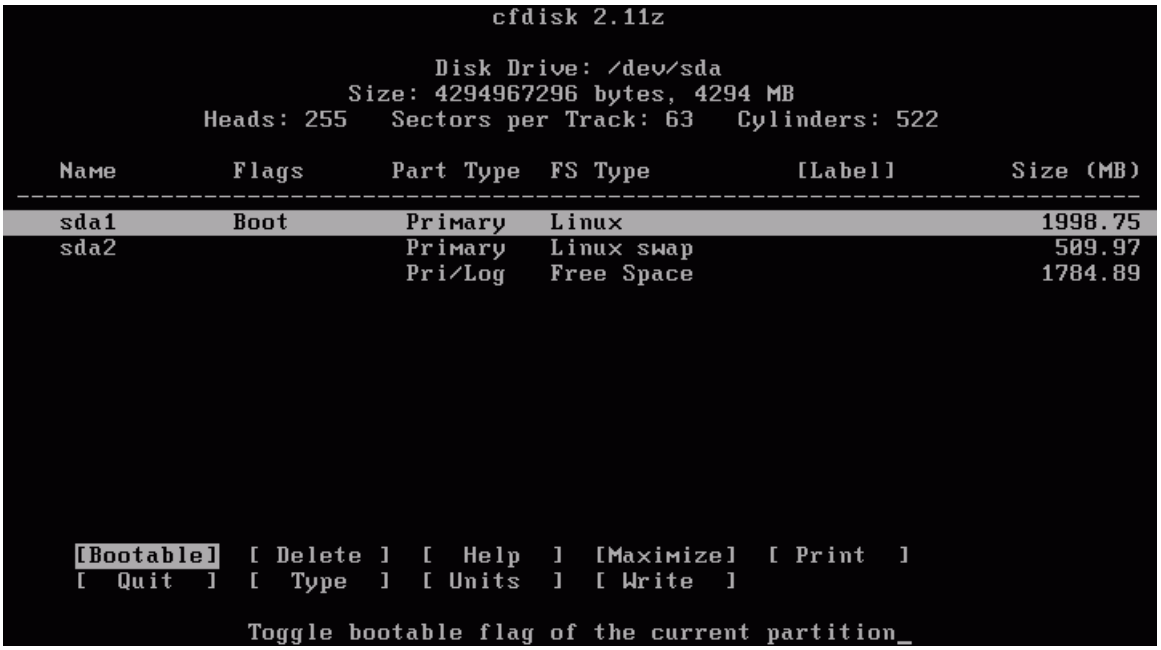
6. The keyboard map defaults to U.S. You may choose a different map at this point if necessary, otherwise, skip to the next step.
7. Use the arrow keys to highlight “Start the Installation Process” and press Enter.

8. Partition your hard disks by choosing the appropriate disk and pressing Enter. If no partition table exists on this disk, you may see the following screen.

9. If this screen is displayed, type “y” and press Enter to start with a blank table.

10. If your hard disk has existing partitions, it is recommended that you delete all of the existing partitions:
    - Use the arrow keys to highlight each existing partition and press “D” to delete it.
11. You will need two partitions, at a minimum, to get started. One partition will be a Linux partition and the other will be a *Linux* Swap partition.
    - Highlight the "Free Space" line and press “N” for New.
    - Choose "Primary" (or "Logical," which works fine too).

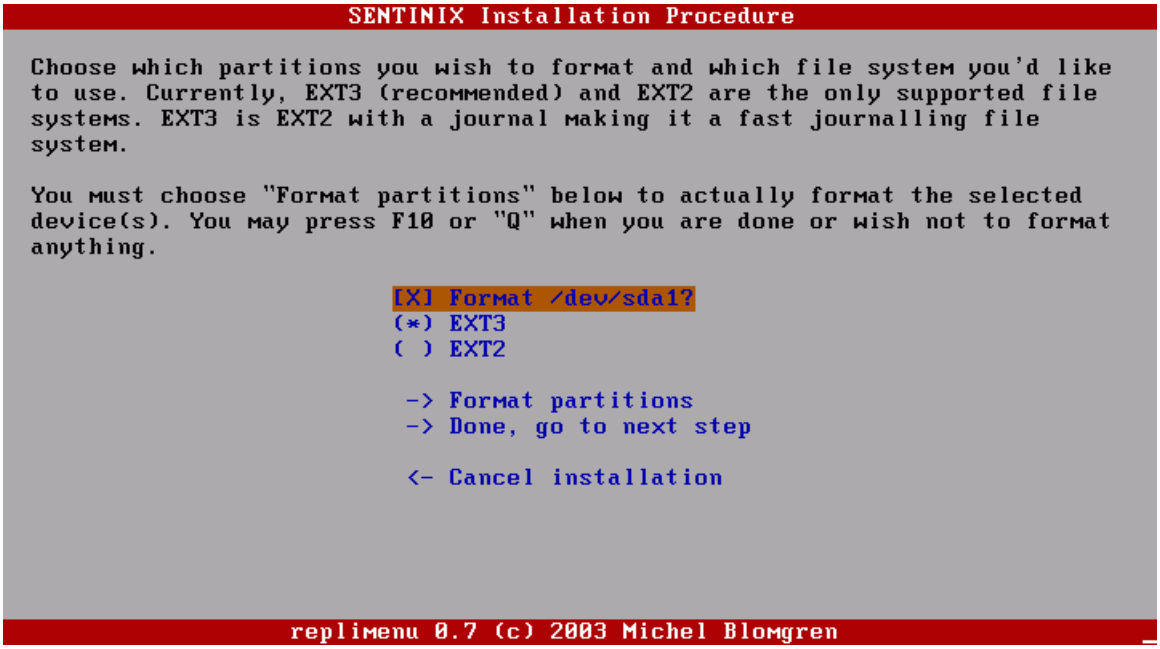
- Make it at least 2GB (type "2000" in the field). You need at least 100MB of free space to create the swap partition later.
- Choose "Beginning."
- Press “T” to select partition type (if it isn't already of type "Linux").
- Type “83” in the "Enter filesystem type:" field.
- Move the focus to "Free Space" and press “N” again.
- Choose "Primary."
- Make it at least 512MB (type "512" in the field).
- Press “T.”
- In the "Enter filesystem type:" field, type "82" (for Linux Swap).
- Move the focus back to the first "Linux" partition and press “B” to mark it "bootable."



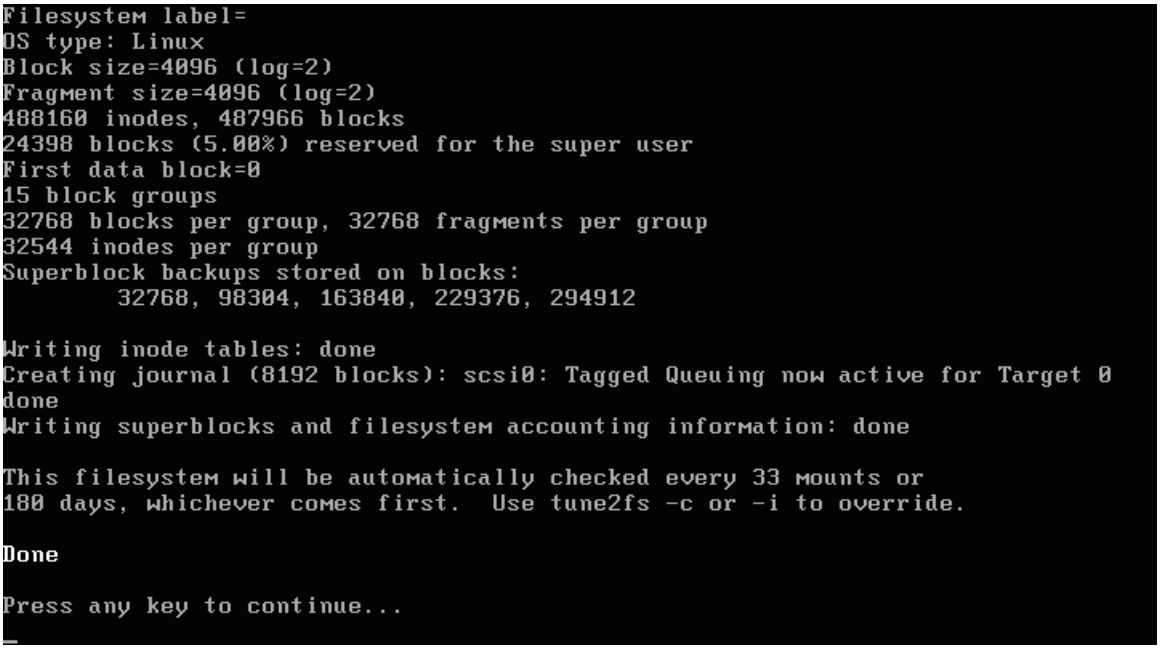
- Your screen should look like the above screenshot.

- Press “W” and type "yes" to write the partition table.
- Press “Q” to quit.

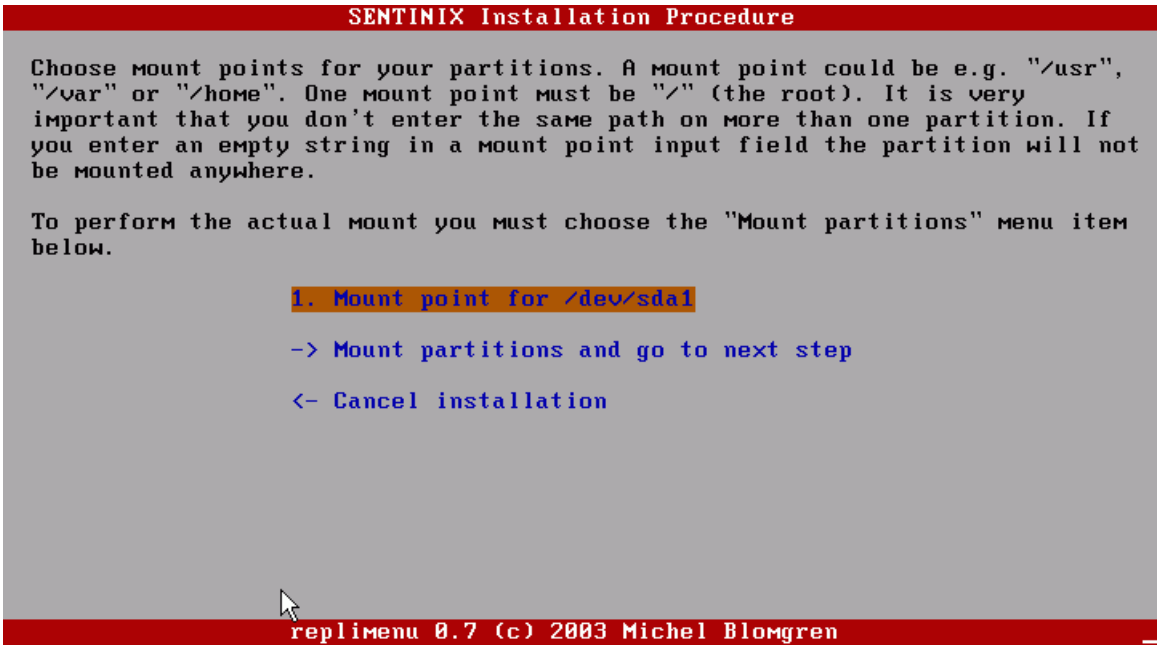
12. Choose "Continue to next step" when you are done partitioning.



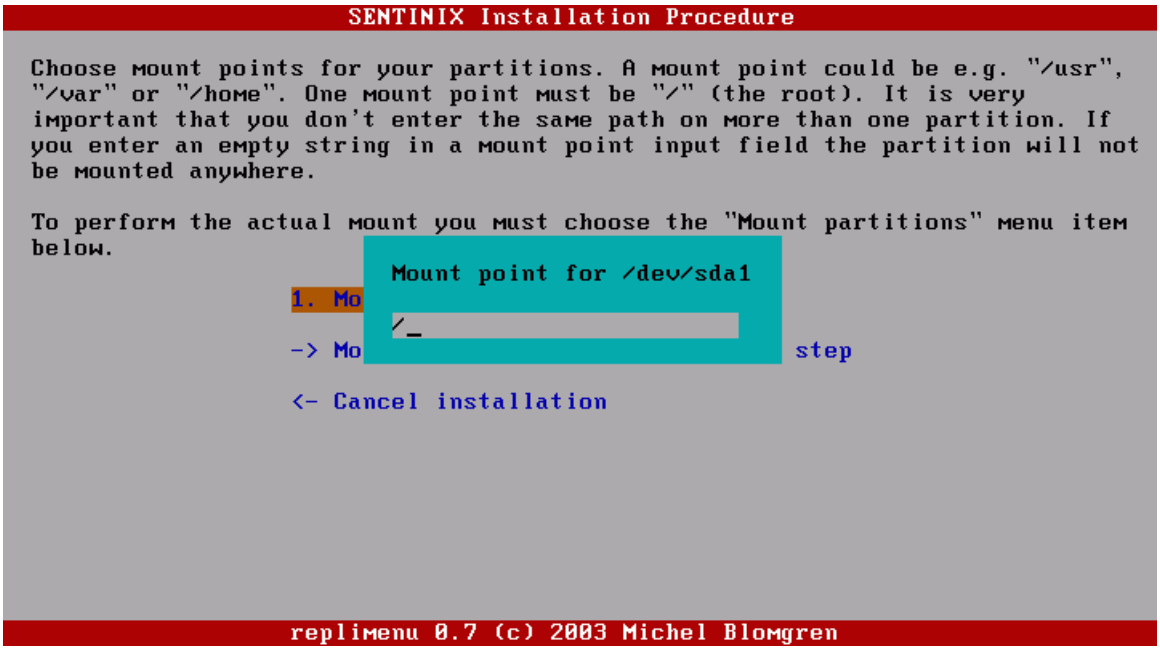
13. Choose the partitions that should be formatted and which file system to use. EXT3 is recommended on all partitions. Choose "Format partitions" to start.



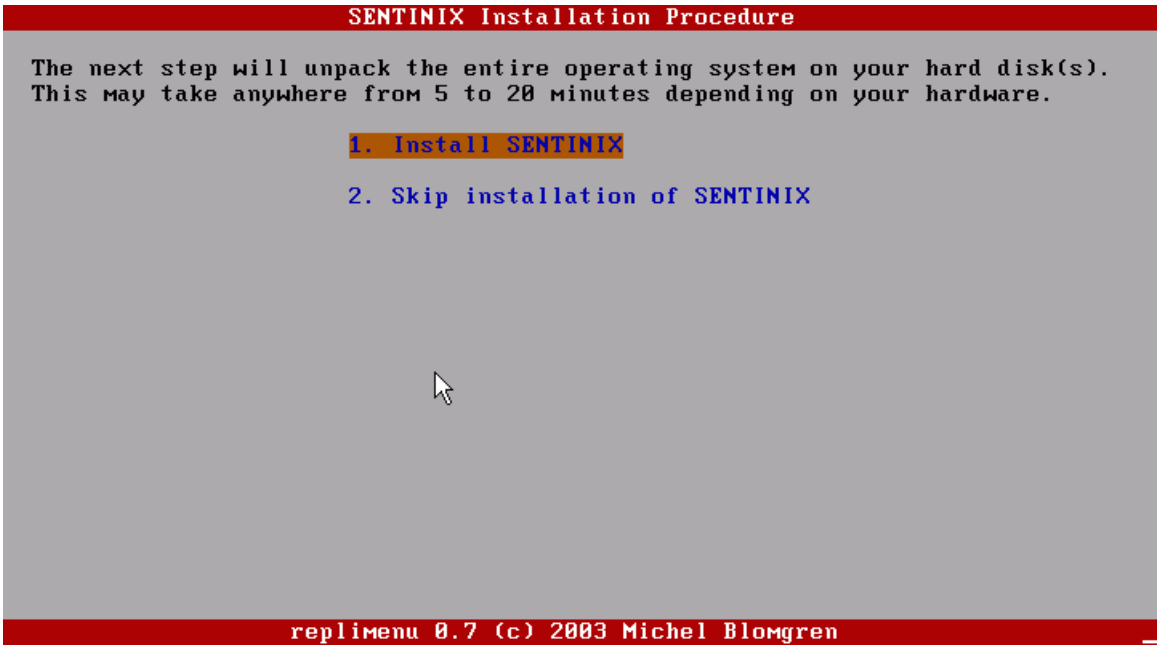
14. When formatting is complete, press any key to return to the previous screen.
15. Choose "Done, go to next step."



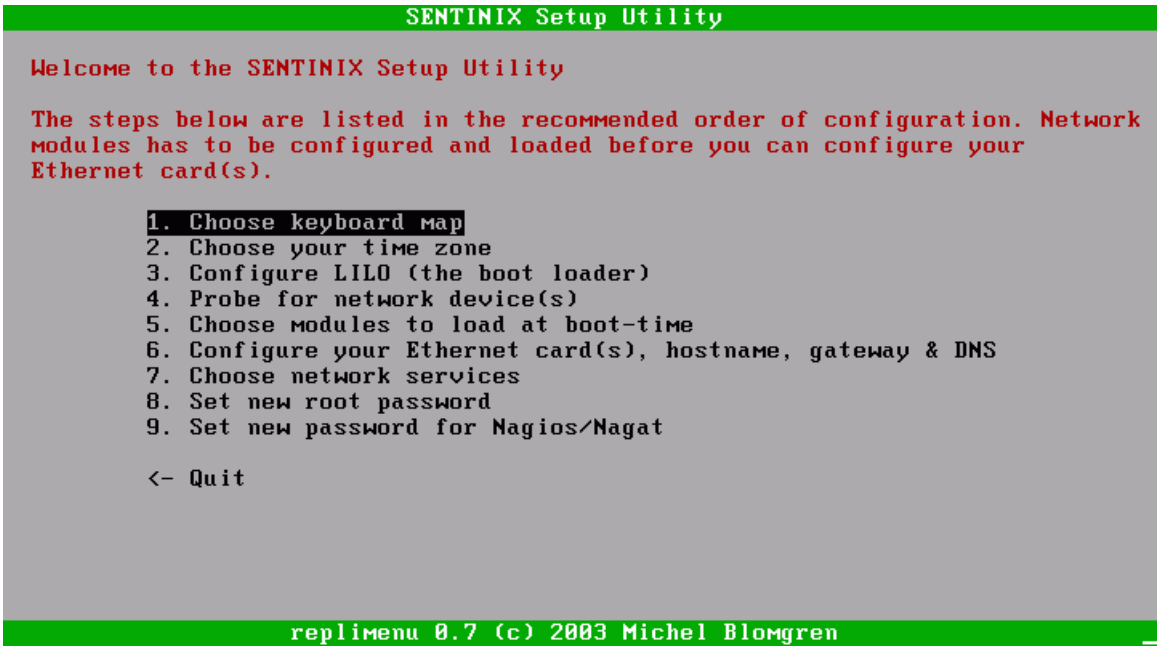
16. You must now set the mount point for your newly formatted volume(s). At least one partition must be mounted to “/” (the root partition). Highlight the desired partition and press Enter.



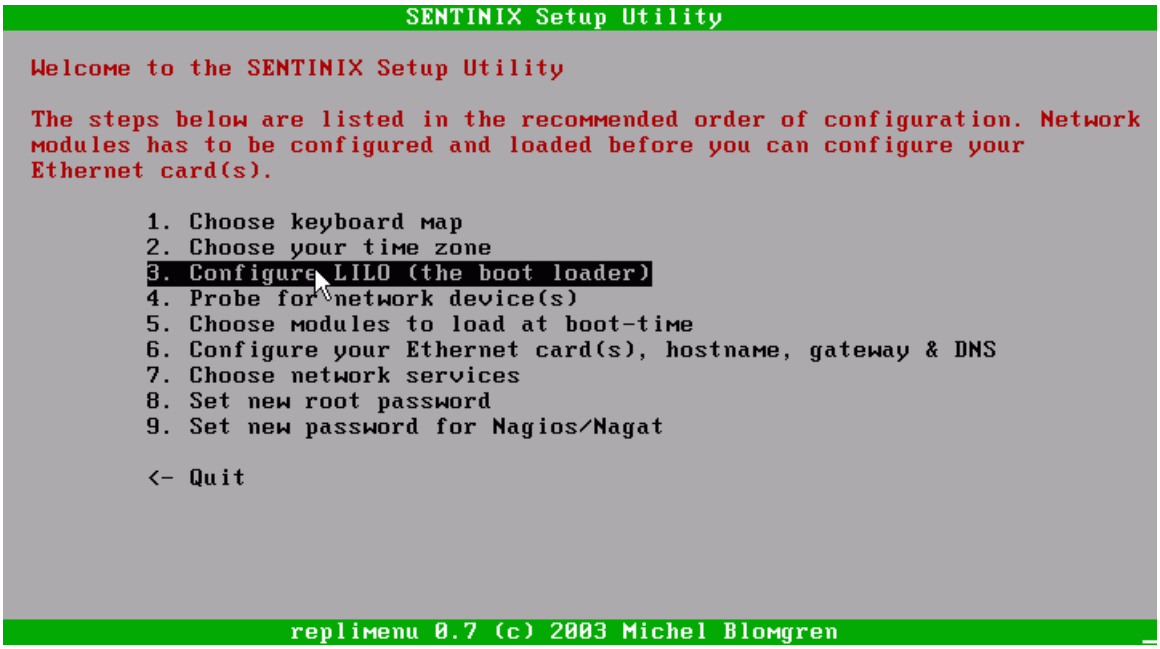
17. Type the desired mount point for this partition. This example shows the setting for the root partition (“/”). Press Enter.



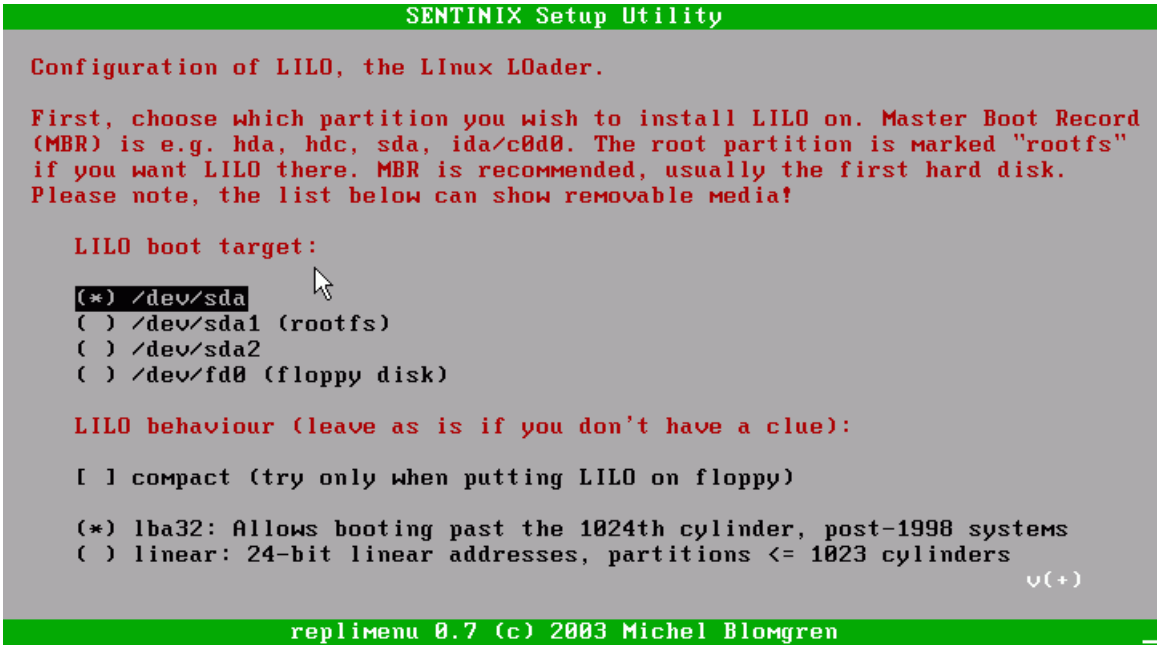
18. Choose "Install SENTINIX" to start the installation. This might take anywhere from 5 minutes to 30 minutes depending on hardware.



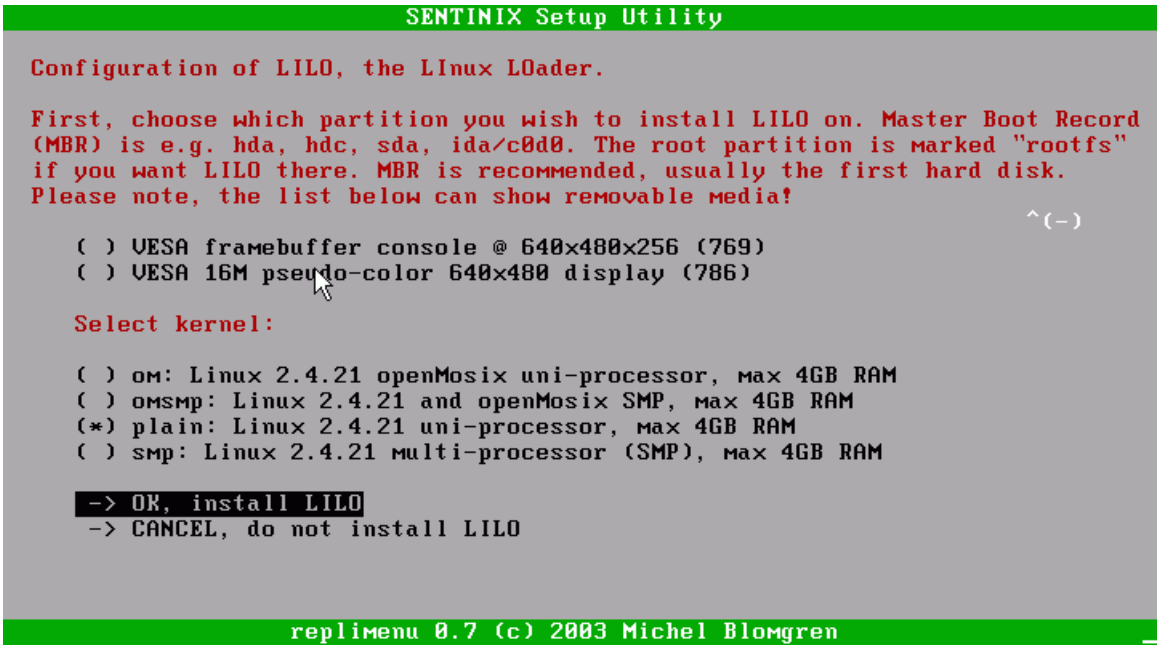
19. If all went well, you should now see a menu titled "SENTINIX Setup Utility." The keyboard map defaults to U.S. If you would like to change the default setting, you may do so at this time. The time zone defaults to GMT. Since we previously set the BIOS clock to GMT time, it is not necessary to change the time zone.



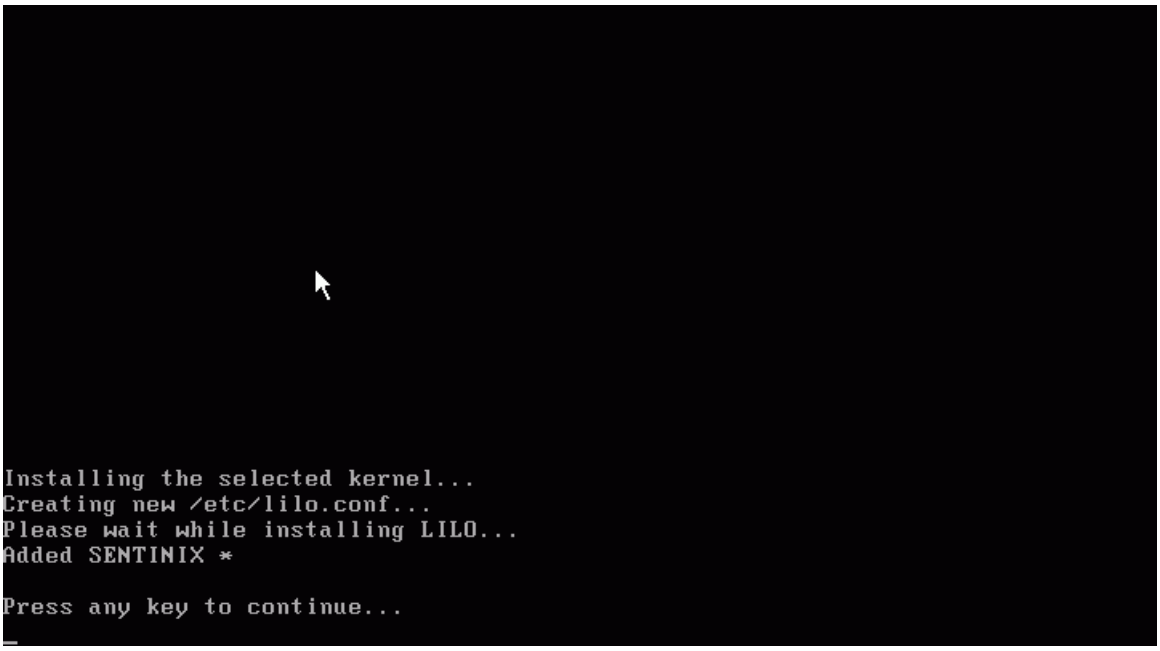
20. Use the down arrow key to move to line 3, “Configure LILO” and press Enter.



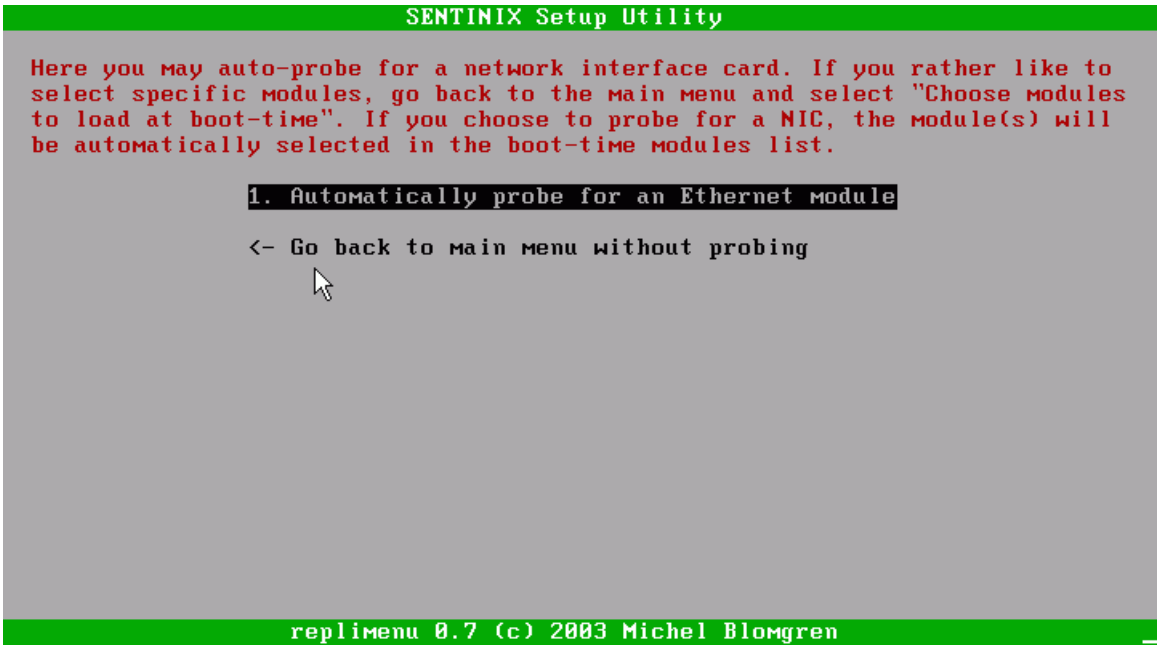
21. LILO is the boot loader for Linux. The defaults should be fine for most installations. The only exception which I am aware is older Compaq hardware that had a “System Partition.” If you are using a machine of this type, you will want to set the boot target to: /dev/hda1 (or /dev/sda1 as shown above for SCSI hardware).



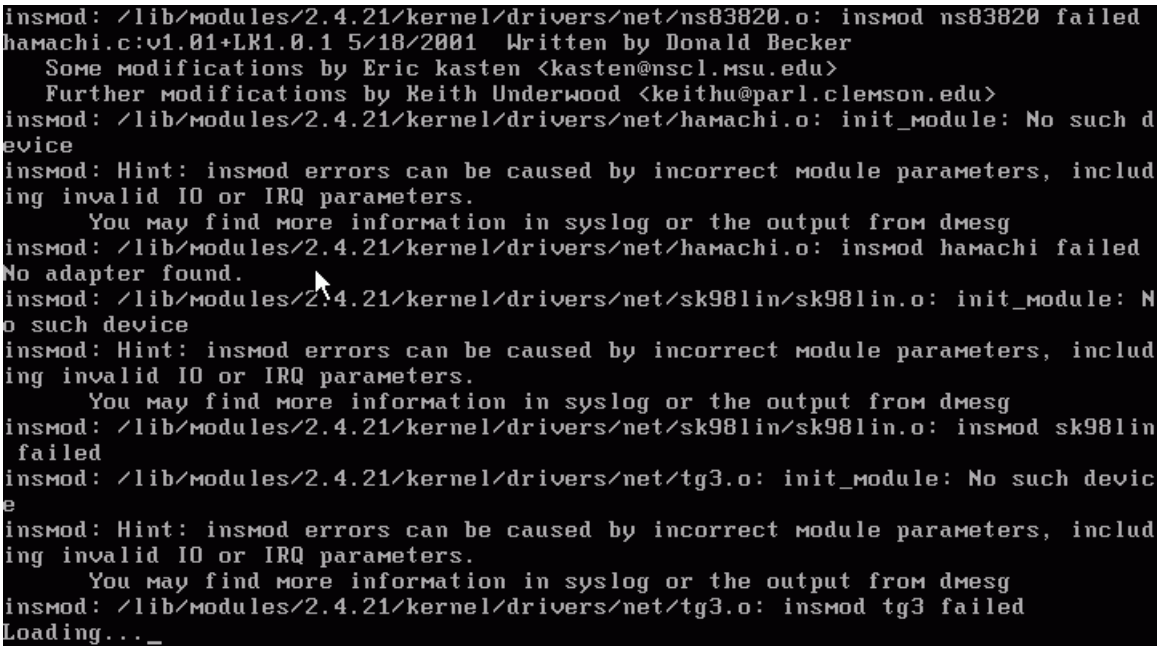
22. Scroll down to “OK, install LILO” and press Enter.



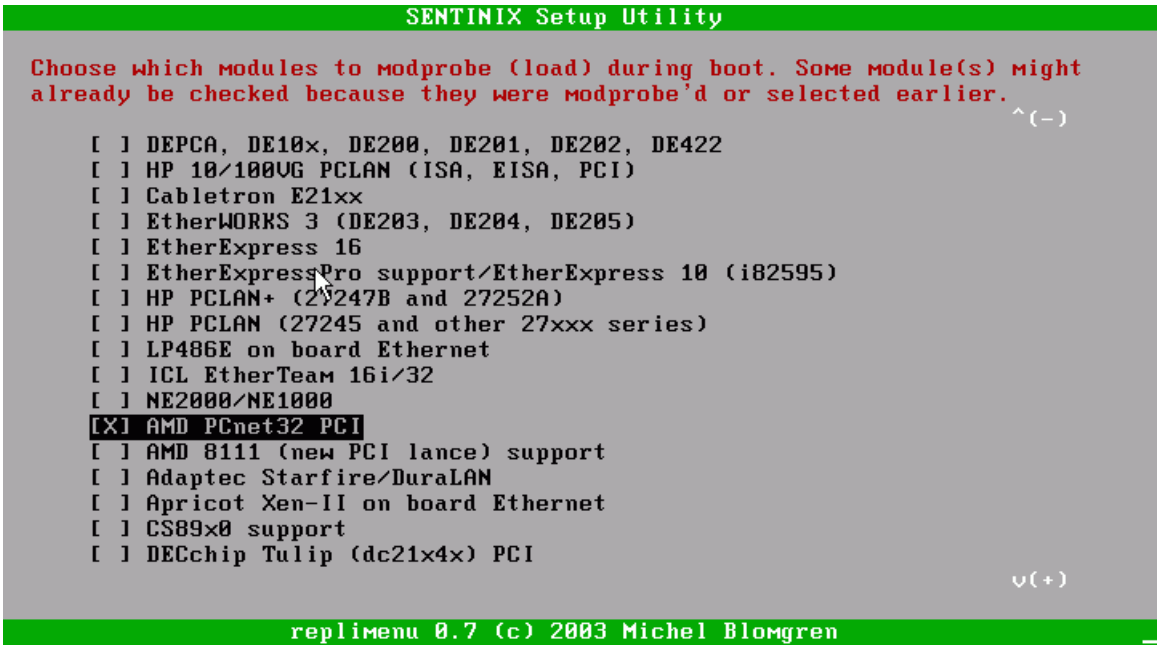
23. LILO is now installed. Press any key to return to the menu and select 4 to probe for network devices.



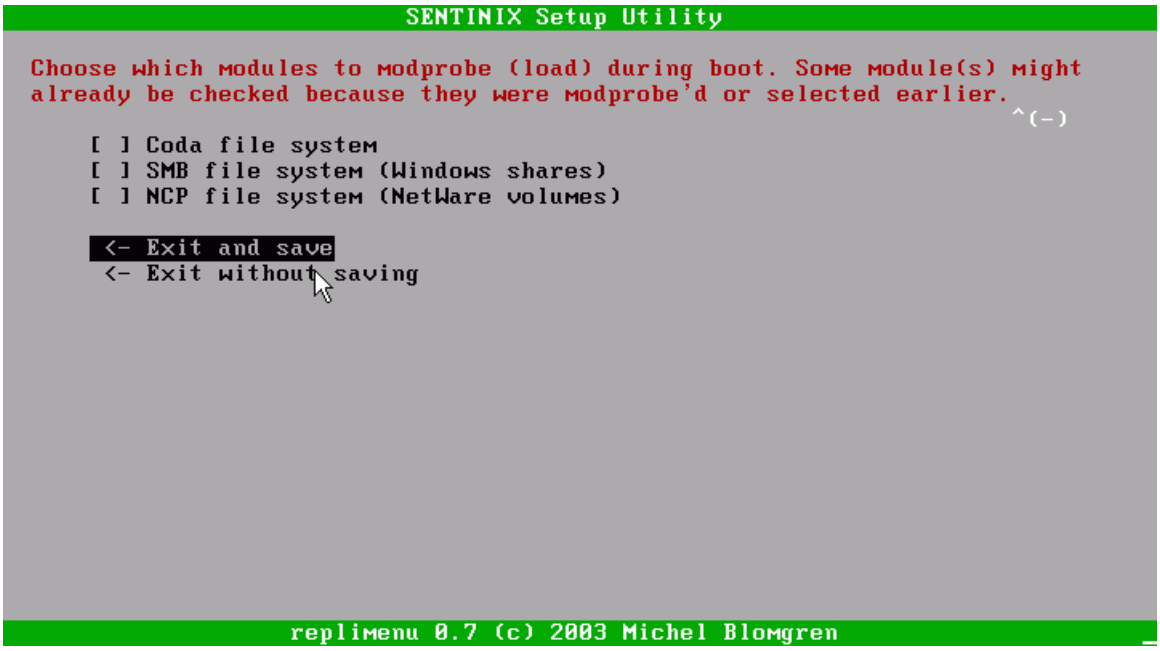
24. Press Enter to probe for Ethernet hardware.



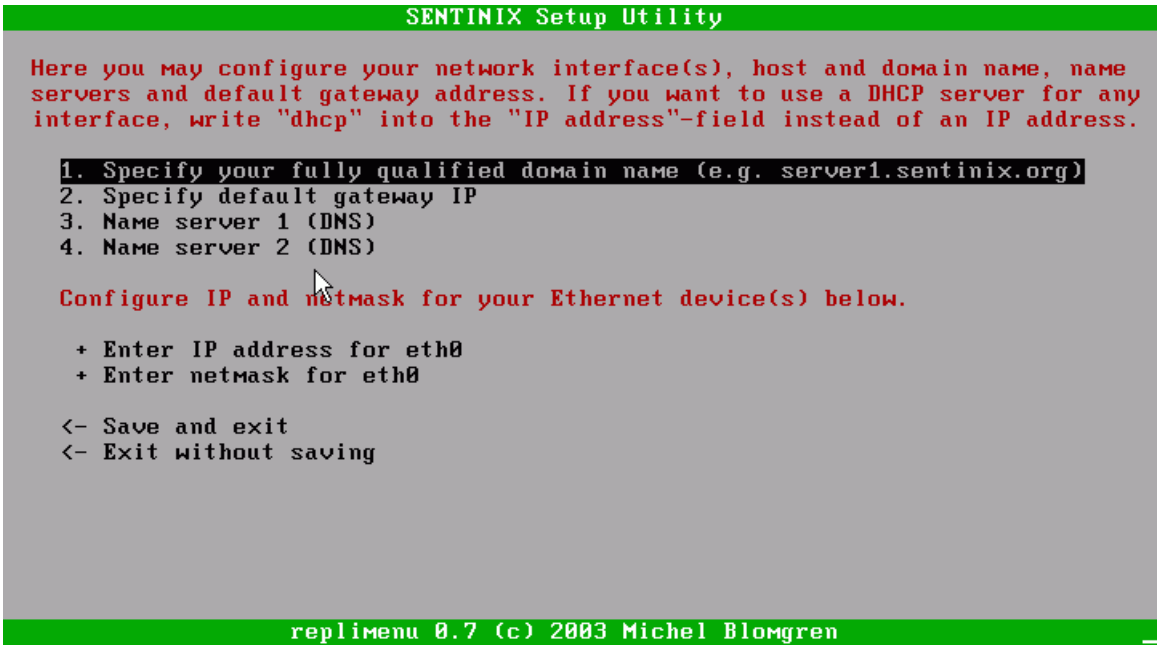
25. Once an appropriate driver (or drivers) is found, they will be loaded and the following screen will appear.



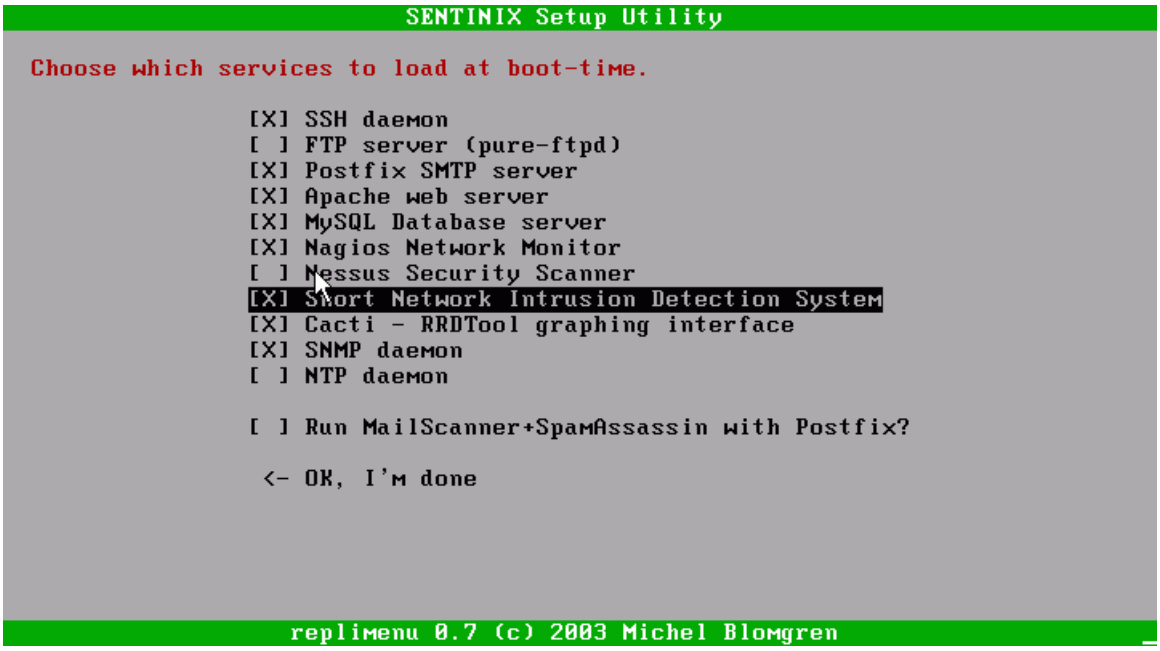
26. Note that the detected card(s) are already selected.



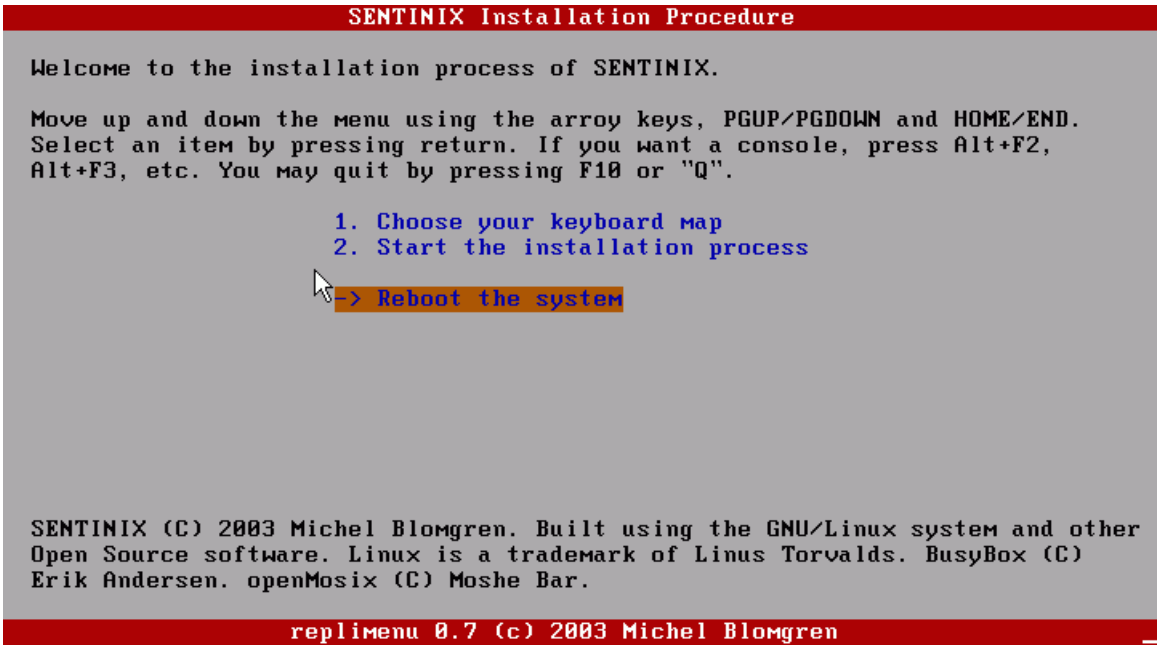
27. Scroll down to “Exit and Save” and press Enter to go back to the menu. You may skip option 5 as the correct modules will already be selected. Choose option 6 to set your network parameters.



28. Beginning with option 1, choose each option and provide the appropriate information. It is not necessary to provide two name servers, although it is a good idea. After setting the name server(s), proceed to the lower section of the screen and set the IP addresses and netmasks for each Ethernet adapter.
29. Choose “Save and Exit” to return to the menu. Choose option 7 to set up network services.



30. Snort will be unchecked. Highlight this line and press the space bar to select Snort. If you wish, you can also add Nessus Security Scanner and NTP daemon.
31. Choose “OK, I’m done” to return to the main menu.
32. By default, the root password is set to “sentinix.” You may use options 8 to reset your root password.
33. Select “Quit” to exit the setup program and return to the installation program.



34. Select “Reboot the system” and press Enter. The CD should be ejected. If the CD does not eject, remove it before the machine begins booting.

Congratulations! You have just completed the installation of your first Snort IDS. If you need to reconfigure your system at any time, log in as root and type "setup."

Getting Started With Snort

If all went well, your Snort system is up and running – already detecting errant probes, port-scans and worm propagation traffic. To see the status of your snort sensor(s), fire up a Web browser and point it to your machine’s IP address. Click on the *Snort Center* link at the top of the screen and log in with the following credentials.

Username: admin
Password: change

SnortCenter displays a list of all of your sensors along with their status. From SnortCenter, you can start, stop and reconfigure your sensors. Figure 2 shows a typical SnortCenter console. If your sensor is highlighted yellow, click on the *Start* link to start the sensor.

Alert data is accessible via the Analysis Console for Intrusion Databases (ACID), which is integrated into SnortCenter. Click on *Alert Console* to go to the ACID summary page (shown in Figure 3). Detailed alert information is available via the *Snapshots* drop-down menu. Figure 4 shows a typical page of sensor detail.

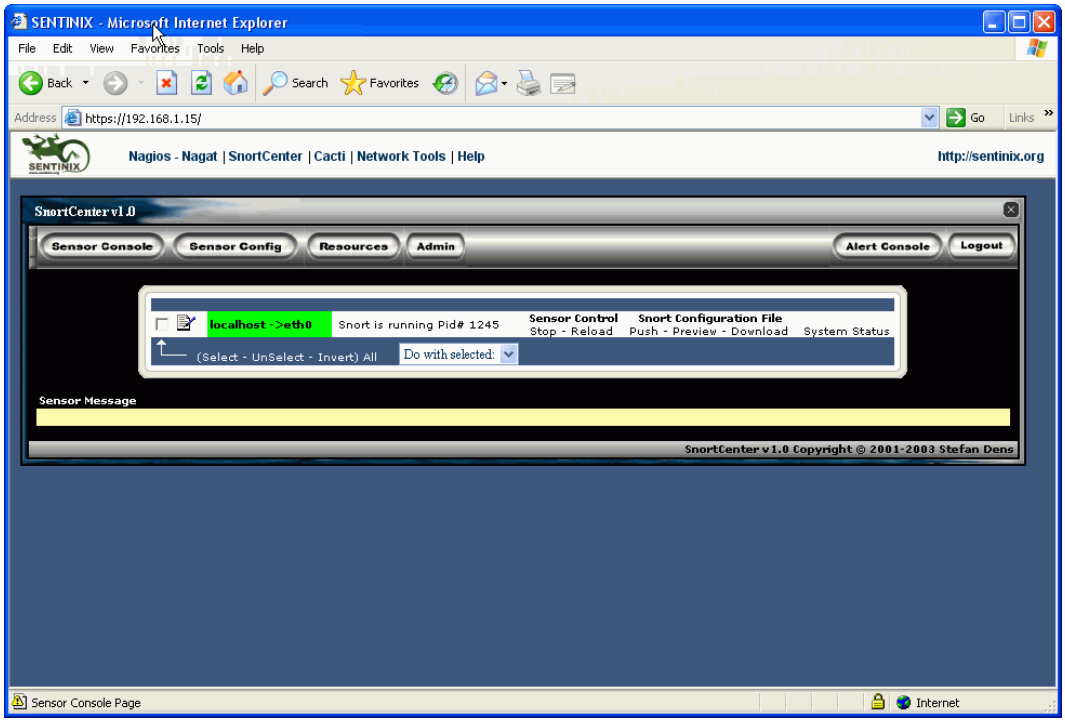


Figure 2 - SnortCenter Console

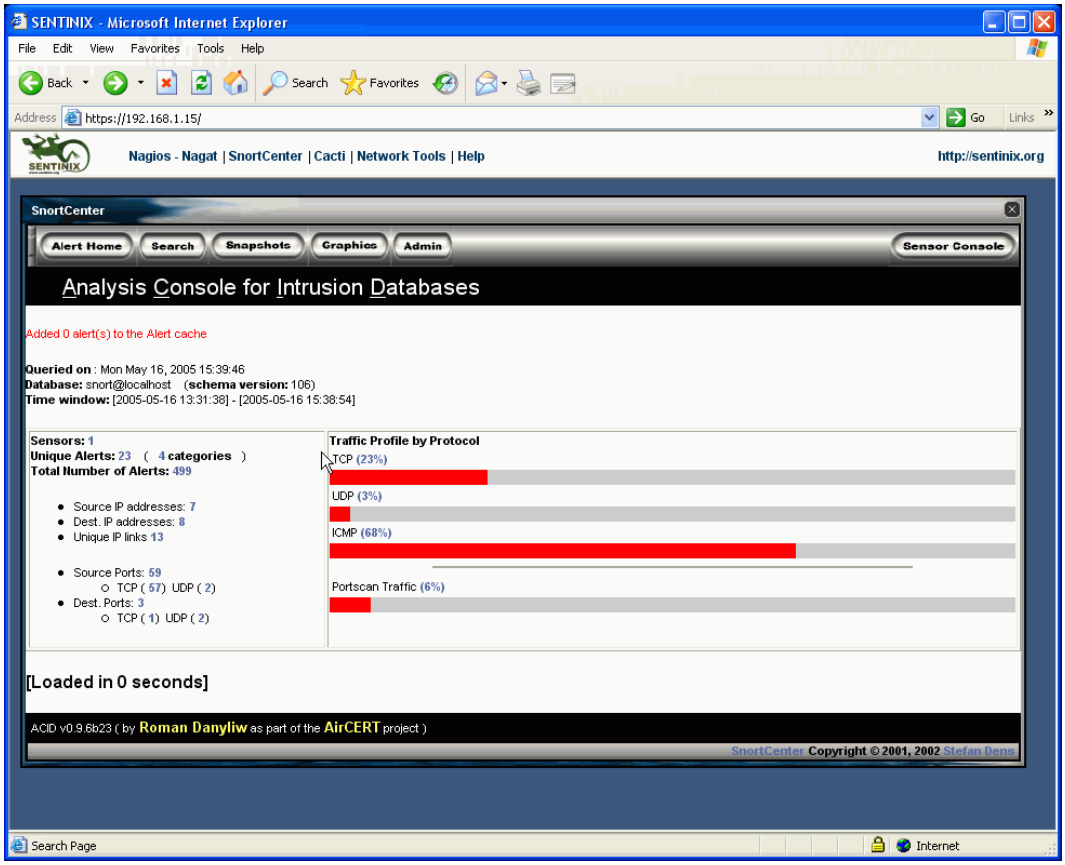
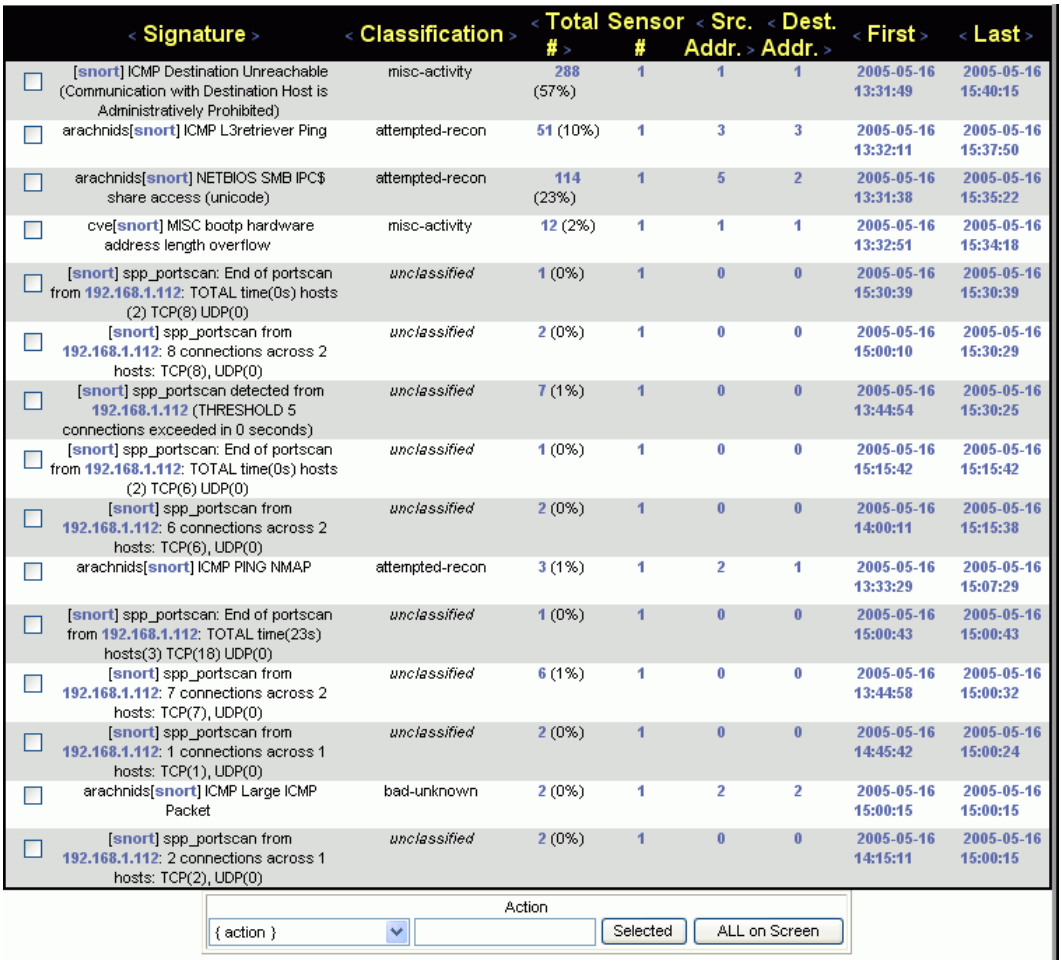


Figure 3 - ACID Summary Page



Signature	Classification	Total #	Sensor #	Src. Addr.	Dest. Addr.	First	Last
[snort] ICMP Destination Unreachable (Communication with Destination Host is Administratively Prohibited)	misc-activity	288 (57%)	1	1	1	2005-05-16 13:31:49	2005-05-16 15:40:15
arachnids[snort] ICMP L3retriever Ping	attempted-recon	51 (10%)	1	3	3	2005-05-16 13:32:11	2005-05-16 15:37:50
arachnids[snort] NETBIOS SMB IPC$ share access (unicode)	attempted-recon	114 (23%)	1	5	2	2005-05-16 13:31:38	2005-05-16 15:35:22
cve[snort] MISC bootp hardware address length overflow	misc-activity	12 (2%)	1	1	1	2005-05-16 13:32:51	2005-05-16 15:34:18
[snort] spp_portscan: End of portscan from 192.168.1.112: TOTAL time(0s) hosts (2) TCP(8) UDP(0)	*unclassified*	1 (0%)	1	0	0	2005-05-16 15:30:39	2005-05-16 15:30:39
[snort] spp_portscan from 192.168.1.112: 8 connections across 2 hosts: TCP(8), UDP(0)	*unclassified*	2 (0%)	1	0	0	2005-05-16 15:00:10	2005-05-16 15:30:29
[snort] spp_portscan detected from 192.168.1.112 (THRESHOLD 5 connections exceeded in 0 seconds)	*unclassified*	7 (1%)	1	0	0	2005-05-16 13:44:54	2005-05-16 15:30:25
[snort] spp_portscan: End of portscan from 192.168.1.112: TOTAL time(0s) hosts (2) TCP(6) UDP(0)	*unclassified*	1 (0%)	1	0	0	2005-05-16 15:15:42	2005-05-16 15:15:42
[snort] spp_portscan from 192.168.1.112: 6 connections across 2 hosts: TCP(6), UDP(0)	*unclassified*	2 (0%)	1	0	0	2005-05-16 14:00:11	2005-05-16 15:15:38
arachnids[snort] ICMP PING NMAP	attempted-recon	3 (1%)	1	2	1	2005-05-16 13:33:29	2005-05-16 15:07:29
[snort] spp_portscan: End of portscan from 192.168.1.112: TOTAL time(23s) hosts(3) TCP(18) UDP(0)	*unclassified*	1 (0%)	1	0	0	2005-05-16 15:00:43	2005-05-16 15:00:43
[snort] spp_portscan from 192.168.1.112: 7 connections across 2 hosts: TCP(7), UDP(0)	*unclassified*	6 (1%)	1	0	0	2005-05-16 13:44:58	2005-05-16 15:00:32
[snort] spp_portscan from 192.168.1.112: 1 connections across 1 hosts: TCP(1), UDP(0)	*unclassified*	2 (0%)	1	0	0	2005-05-16 14:45:42	2005-05-16 15:00:24
arachnids[snort] ICMP Large ICMP Packet	bad-unknown	2 (0%)	1	2	2	2005-05-16 15:00:15	2005-05-16 15:00:15
[snort] spp_portscan from 192.168.1.112: 2 connections across 1 hosts: TCP(2), UDP(0)	*unclassified*	2 (0%)	1	0	0	2005-05-16 14:15:11	2005-05-16 15:00:15

Figure 4 - Sensor Detail Snapshot

Continuing On

Sentinix provides a convenient platform to get a Snort IDS up and running. It is important to remember, however, that an IDS is not a set-and-forget system. IDSs must be kept up to date and monitored. In fact, one of the first things you should do if you decide to make Snort part of your security solution is update the latest versions of Snort and Snort's signatures. Initially, there will be a large number of nuisance alerts. Careful tuning of rules will help reduce the amount of noise while maintaining the overall integrity of the IDS.

Other Resources

A number of resources are available to help you create an industrial strength Snort setup that is customized for your particular business.

- Snort 2.1 Intrusion Detection – an excellent text and reference published by Syngress.
- www.snort.org – for the latest software, documentation and other resources.
- Snort GUI for Lamers (SGUIL) – an alternative configuration interface.
- Barnyard - alert post-processing for larger installations.
- Sourcefire – commercial support.

Sentinix Extras

Sentinix includes a number of other useful tools you may want to explore. These include:

- Nagios – Server Health Monitoring
- Nessus – Heavy-Duty Security Testing
- RRDTool, Cacti – Performance Graphing