

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>.

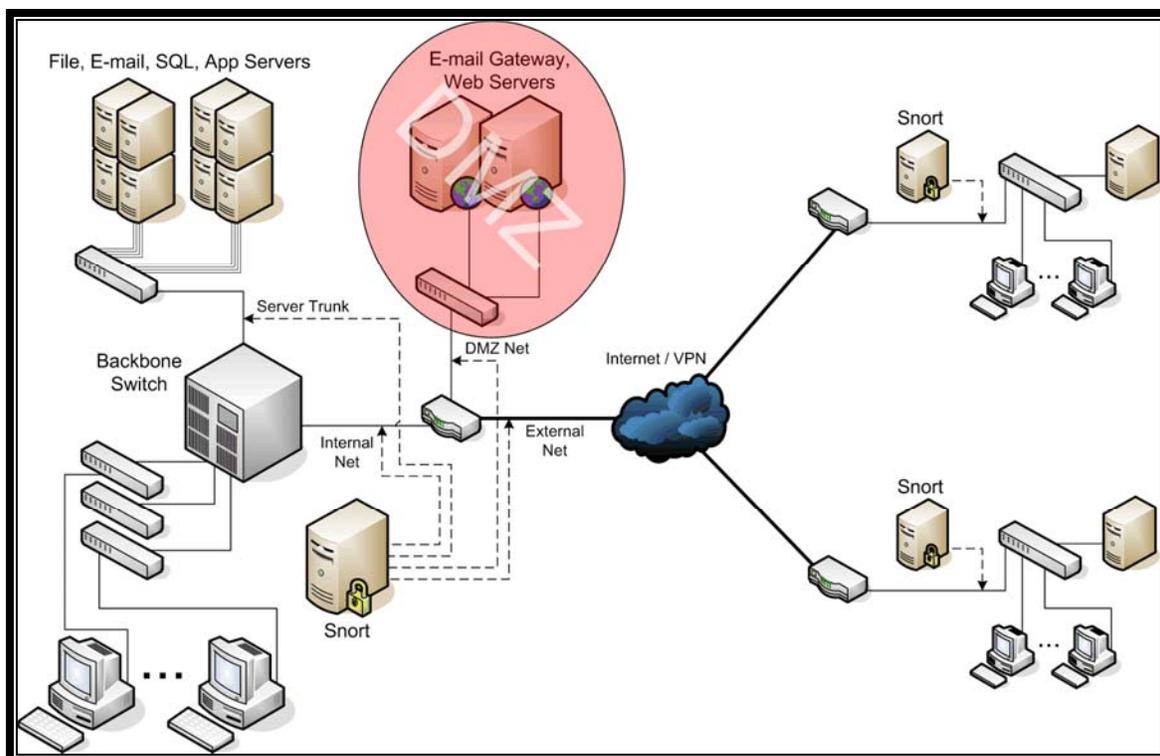


Figure 1 - Placement of Snort Sensors

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.

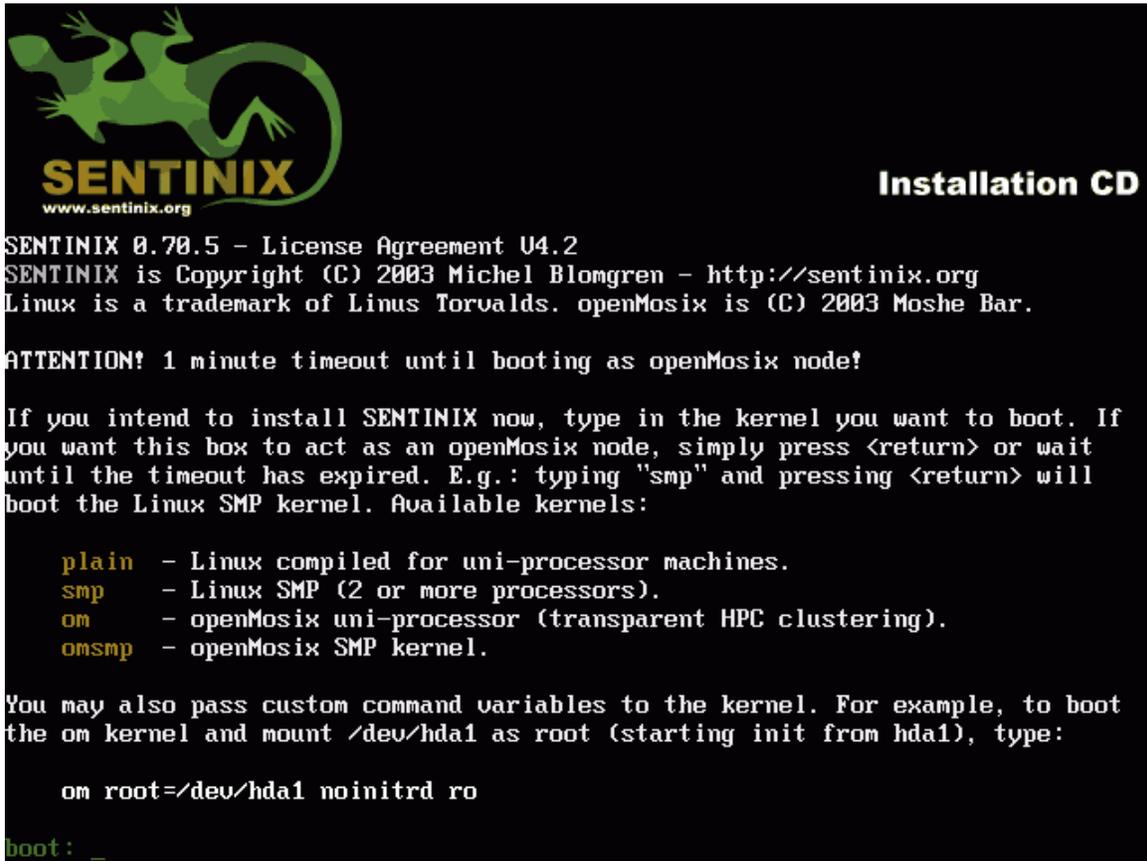
Installing Sentinix

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!



The image shows the boot screen of the SENTINIX Installation CD. At the top left is the SENTINIX logo, which features a green dragon-like creature and the text 'SENTINIX' with the website 'www.sentinix.org' below it. To the right of the logo, the text 'Installation CD' is displayed. Below the logo, the following text is shown: 'SENTINIX 0.70.5 - License Agreement U4.2', 'SENTINIX is Copyright (C) 2003 Michel Blomgren - http://sentinix.org', and 'Linux is a trademark of Linus Torvalds. openMosix is (C) 2003 Moshe Bar.' A warning message reads: 'ATTENTION! 1 minute timeout until booting as openMosix node!'. Below this, instructions are provided: 'If you intend to install SENTINIX now, type in the kernel you want to boot. If you want this box to act as an openMosix node, simply press <return> or wait until the timeout has expired. E.g.: typing "smp" and pressing <return> will boot the Linux SMP kernel. Available kernels:'. A list of kernels follows: 'plain - Linux compiled for uni-processor machines.', 'smp - Linux SMP (2 or more processors).', 'om - openMosix uni-processor (transparent HPC clustering).', and 'omsmp - openMosix SMP kernel.'. Further instructions state: 'You may also pass custom command variables to the kernel. For example, to boot the om kernel and mount /dev/hda1 as root (starting init from hda1), type:'. A sample command is shown: 'om root=/dev/hda1 noinitrd ro'. At the bottom, the boot prompt 'boot: _' is visible.

```
SENTINIX 0.70.5 - License Agreement U4.2
SENTINIX is Copyright (C) 2003 Michel Blomgren - http://sentinix.org
Linux is a trademark of Linus Torvalds. openMosix is (C) 2003 Moshe Bar.

ATTENTION! 1 minute timeout until booting as openMosix node!

If you intend to install SENTINIX now, type in the kernel you want to boot. If
you want this box to act as an openMosix node, simply press <return> or wait
until the timeout has expired. E.g.: typing "smp" and pressing <return> will
boot the Linux SMP kernel. Available kernels:

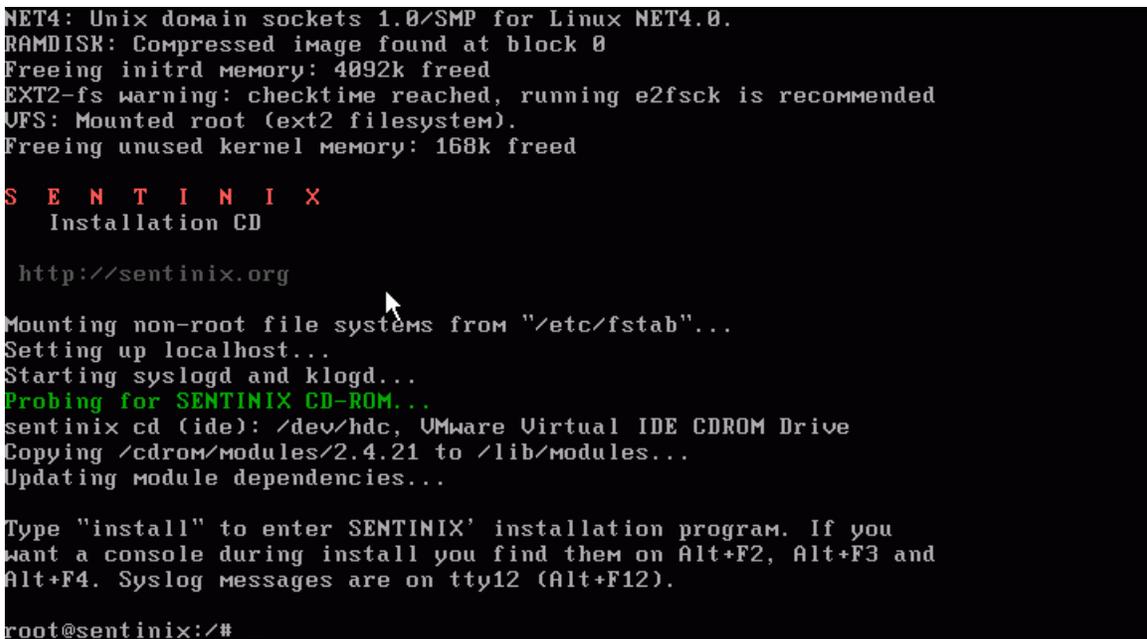
plain - Linux compiled for uni-processor machines.
smp - Linux SMP (2 or more processors).
om - openMosix uni-processor (transparent HPC clustering).
omsmp - openMosix SMP kernel.

You may also pass custom command variables to the kernel. For example, to boot
the om kernel and mount /dev/hda1 as root (starting init from hda1), type:

om root=/dev/hda1 noinitrd ro

boot: _
```

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



The image shows the boot screen of the SENTINIX Installation CD. At the top, the following text is displayed: 'NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.', 'RAMDISK: Compressed image found at block 0', 'Freeing initrd memory: 4092k freed', 'EXT2-fs warning: checktime reached, running e2fsck is recommended', 'UFS: Mounted root (ext2 filesystem).', and 'Freeing unused kernel memory: 168k freed'. Below this, the text 'S E N T I N I X' is displayed in large, spaced-out letters, followed by 'Installation CD'. The website 'http://sentinix.org' is shown. Below this, the following text is displayed: 'Mounting non-root file systems from "/etc/fstab"...', 'Setting up localhost...', 'Starting syslogd and klogd...', 'Probing for SENTINIX CD-ROM...', 'sentinix cd (ide): /dev/hdc, VMware Virtual IDE CDROM Drive', 'Copying /cdrom/modules/2.4.21 to /lib/modules...', and 'Updating module dependencies...'. Further instructions state: 'Type "install" to enter SENTINIX' installation program. If you want a console during install you find them on Alt+F2, Alt+F3 and Alt+F4. Syslog messages are on tty12 (Alt+F12)'. At the bottom, the boot prompt 'root@sentinix:/# _' is visible.

```
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
RAMDISK: Compressed image found at block 0
Freeing initrd memory: 4092k freed
EXT2-fs warning: checktime reached, running e2fsck is recommended
UFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 168k freed

S E N T I N I X
Installation CD

http://sentinix.org

Mounting non-root file systems from "/etc/fstab"...
Setting up localhost...
Starting syslogd and klogd...
Probing for SENTINIX CD-ROM...
sentinix cd (ide): /dev/hdc, VMware Virtual IDE CDROM Drive
Copying /cdrom/modules/2.4.21 to /lib/modules...
Updating module dependencies...

Type "install" to enter SENTINIX' installation program. If you
want a console during install you find them on Alt+F2, Alt+F3 and
Alt+F4. Syslog messages are on tty12 (Alt+F12).

root@sentinix:/# _
```

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

```
SENTINIX Installation Procedure

Welcome to the installation process of SENTINIX.

Move up and down the menu using the array keys, PGUP/PGDOWN and HOME/END.
Select an item by pressing return. If you want a console, press Alt+F2,
Alt+F3, etc. You may quit by pressing F10 or "Q".

1. Choose your keyboard map
2. Start the installation process

-> Reboot the system

SENTINIX (C) 2003 Michel Blomgren. Built using the GNU/Linux system and other
Open Source software. Linux is a trademark of Linus Torvalds. BusyBox (C)
Erik Andersen. openMosix (C) Moshe Bar.

replimenu 0.7 (c) 2003 Michel Blomgren
```

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.

```
SENTINIX Installation Procedure

You may now partition your hard disk(s). Choose which hard disk drive you
wish to edit.

1. /dev/sda

-> Continue to next step
<- Cancel installation

replimenu 0.7 (c) 2003 Michel Blomgren
```

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.

```
No partition table or unknown signature on partition table
Do you wish to start with a zero table [y/N] ?_
```

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

```
          cfdisk 2.11z
          Disk Drive: /dev/sda
          Size: 4294967296 bytes, 4294 MB
          Heads: 255 Sectors per Track: 63 Cylinders: 522
-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
          Pri/Log  Free Space          4293.68
-----
[ Help ] [ New ] [ Print ] [ Quit ] [ Units ]
[ Write ]
          Print help screen_
```

10. If your hard disk has existing partitions, it is recommended that you delete all of the existing partitions:
 - o 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.
 - o Highlight the "Free Space" line and press "N" for New.
 - o Choose "Primary" (or "Logical," which works fine too).

```

cfdisk 2.11z

Disk Drive: /dev/sda
Size: 4294967296 bytes, 4294 MB
Heads: 255 Sectors per Track: 63 Cylinders: 522

Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
                Pri/Log    Free Space          4293.60

Size (in MB): 2000_

```

- 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."

```

cfdisk 2.11z

Disk Drive: /dev/sda
Size: 4294967296 bytes, 4294 MB
Heads: 255 Sectors per Track: 63 Cylinders: 522

Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
sda1      Boot       Primary    Linux         1998.75
sda2                         Primary    Linux swap    509.97
                Pri/Log    Free Space          1784.89

[Bootable] [ Delete ] [ Help ] [Maximize] [ Print ]
[ Quit ] [ Type ] [ Units ] [ Write ]

Toggle bootable flag of the current partition_

```

- 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.

```

SENTINIX Installation Procedure

Choose which partitions you wish to format and which file system you'd like
to use. Currently, EXT3 (recommended) and EXT2 are the only supported file
systems. EXT3 is EXT2 with a journal making it a fast journalling file
system.

You must choose "Format partitions" below to actually format the selected
device(s). You may press F10 or "Q" when you are done or wish not to format
anything.

[X] Format /dev/sda1?
(*) EXT3
( ) EXT2

-> Format partitions
-> Done, go to next step

<- Cancel installation

replimenu 0.7 (c) 2003 Michel Blomgren

```

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.

```

Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
488160 inodes, 487966 blocks
24398 blocks (5.00%) reserved for the super user
First data block=0
15 block groups
32768 blocks per group, 32768 fragments per group
32544 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Creating journal (8192 blocks): scsi0: Tagged Queuing now active for Target 0
done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 33 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.

Done
Press any key to continue...

```

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

SENTINIX Installation Procedure

Choose mount points for your partitions. A mount point could be e.g. "/usr", "/var" or "/home". One mount point must be "/" (the root). It is very important that you don't enter the same path on more than one partition. If you enter an empty string in a mount point input field the partition will not be mounted anywhere.

To perform the actual mount you must choose the "Mount partitions" menu item below.

1. Mount point for /dev/sda1

-> Mount partitions and go to next step

<- Cancel installation

replimenu 0.7 (c) 2003 Michel Blomgren

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.

SENTINIX Installation Procedure

Choose mount points for your partitions. A mount point could be e.g. "/usr", "/var" or "/home". One mount point must be "/" (the root). It is very important that you don't enter the same path on more than one partition. If you enter an empty string in a mount point input field the partition will not be mounted anywhere.

To perform the actual mount you must choose the "Mount partitions" menu item below.

Mount point for /dev/sda1

1. Mo

-> Mo / step

<- Cancel installation

replimenu 0.7 (c) 2003 Michel Blomgren

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

SENTINIX Installation Procedure

The next step will unpack the entire operating system on your hard disk(s). This may take anywhere from 5 to 20 minutes depending on your hardware.

1. Install SENTINIX

2. Skip installation of SENTINIX



replimenu 0.7 (c) 2003 Michel Blomgren

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

SENTINIX Setup Utility

Welcome to the SENTINIX Setup Utility

The steps below are listed in the recommended order of configuration. Network modules has to be configured and loaded before you can configure your Ethernet card(s).

- 1. Choose keyboard map**
2. Choose your time zone
3. Configure LILO (the boot loader)
4. Probe for network device(s)
5. Choose modules to load at boot-time
6. Configure your Ethernet card(s), hostname, gateway & DNS
7. Choose network services
8. Set new root password
9. Set new password for Nagios/Nagat

<- Quit

replimenu 0.7 (c) 2003 Michel Blomgren

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.

```
SENTINIX Setup Utility

Welcome to the SENTINIX Setup Utility

The steps below are listed in the recommended order of configuration. Network
modules has to be configured and loaded before you can configure your
Ethernet card(s).

1. Choose keyboard map
2. Choose your time zone
3. Configure LILO (the boot loader)
4. Probe for network device(s)
5. Choose modules to load at boot-time
6. Configure your Ethernet card(s), hostname, gateway & DNS
7. Choose network services
8. Set new root password
9. Set new password for Nagios/Nagat

<- Quit

replimenu 0.7 (c) 2003 Michel Blomgren
```

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

```
SENTINIX Setup Utility

Configuration of LILO, the LInux LOader.

First, choose which partition you wish to install LILO on. Master Boot Record
(MBR) is e.g. hda, hdc, sda, ida/c0d0. The root partition is marked "rootfs"
if you want LILO there. MBR is recommended, usually the first hard disk.
Please note, the list below can show removable media!

LILo boot target:
(*) /dev/sda
( ) /dev/sda1 (rootfs)
( ) /dev/sda2
( ) /dev/fd0 (floppy disk)

LILo behaviour (leave as is if you don't have a clue):

[ ] compact (try only when putting LILo on floppy)

(*) lba32: Allows booting past the 1024th cylinder, post-1998 systems
( ) linear: 24-bit linear addresses, partitions <= 1023 cylinders

replimenu 0.7 (c) 2003 Michel Blomgren
```

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).

```
SENTINIX Setup Utility

Configuration of LILO, the Linux LOader.

First, choose which partition you wish to install LILO on. Master Boot Record
(MBR) is e.g. hda, hdc, sda, ida/c0d0. The root partition is marked "rootfs"
if you want LILO there. MBR is recommended, usually the first hard disk.
Please note, the list below can show removable media!

( ) VESA framebuffer console @ 640x480x256 (769)
( ) VESA 16M pseudo-color 640x480 display (786)

Select kernel:

( ) om: Linux 2.4.21 openMosix uni-processor, max 4GB RAM
( ) omsmp: Linux 2.4.21 and openMosix SMP, max 4GB RAM
(*) plain: Linux 2.4.21 uni-processor, max 4GB RAM
( ) smp: Linux 2.4.21 multi-processor (SMP), max 4GB RAM

-> OK, install LILO
-> CANCEL, do not install LILO

replimenu 0.7 (c) 2003 Michel Blomgren
```

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

```
Installing the selected kernel...
Creating new /etc/lilo.conf...
Please wait while installing LILO...
Added SENTINIX *

Press any key to continue...
```

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

SENTINIX Setup Utility

Here you may auto-probe for a network interface card. If you rather like to select specific modules, go back to the main menu and select "Choose modules to load at boot-time". If you choose to probe for a NIC, the module(s) will be automatically selected in the boot-time modules list.

1. Automatically probe for an Ethernet module

<- Go back to main menu without probing



replimenu 0.7 (c) 2003 Michel Blomgren

24. Press Enter to probe for Ethernet hardware.

```
insmod: /lib/modules/2.4.21/kernel/drivers/net/ns83820.o: insmod ns83820 failed
hamachi.c:v1.01+LK1.0.1 5/18/2001  Written by Donald Becker
  Some modifications by Eric kasten <kasten@nscl.msu.edu>
  Further modifications by Keith Underwood <keithu@parl.clemson.edu>
insmod: /lib/modules/2.4.21/kernel/drivers/net/hamachi.o: init_module: No such device
insmod: Hint: insmod errors can be caused by incorrect module parameters, including invalid IO or IRQ parameters.
  You may find more information in syslog or the output from dmesg
insmod: /lib/modules/2.4.21/kernel/drivers/net/hamachi.o: insmod hamachi failed
No adapter found.
insmod: /lib/modules/2.4.21/kernel/drivers/net/sk98lin/sk98lin.o: init_module: No such device
insmod: Hint: insmod errors can be caused by incorrect module parameters, including invalid IO or IRQ parameters.
  You may find more information in syslog or the output from dmesg
insmod: /lib/modules/2.4.21/kernel/drivers/net/sk98lin/sk98lin.o: insmod sk98lin failed
insmod: /lib/modules/2.4.21/kernel/drivers/net/tg3.o: init_module: No such device
insmod: Hint: insmod errors can be caused by incorrect module parameters, including invalid IO or IRQ parameters.
  You may find more information in syslog or the output from dmesg
insmod: /lib/modules/2.4.21/kernel/drivers/net/tg3.o: insmod tg3 failed
Loading..._
```

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

```
SENTINIX Setup Utility

Choose which modules to modprobe (load) during boot. Some module(s) might
already be checked because they were modprobe'd or selected earlier.      ^(-)

[ ] DEPCA, DE10x, DE200, DE201, DE202, DE422
[ ] HP 10/100VG PCLAN (ISA, EISA, PCI)
[ ] Cabletron E21xx
[ ] EtherWORKS 3 (DE203, DE204, DE205)
[ ] EtherExpress 16
[ ] EtherExpressPro support/EtherExpress 10 (i82595)
[ ] HP PCLAN+ (27247B and 27252A)
[ ] HP PCLAN (27245 and other 27xxx series)
[ ] LP486E on board Ethernet
[ ] ICL EtherTeam 16i/32
[ ] NE2000/NE1000
[X] AMD PCnet32 PCI
[ ] AMD 8111 (new PCI lance) support
[ ] Adaptec Starfire/DuraLAN
[ ] Apricot Xen-II on board Ethernet
[ ] CS89x0 support
[ ] DECchip Tulip (dc21x4x) PCI                                          v(+)
```

replimenu 0.7 (c) 2003 Michel Blomgren

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

```
SENTINIX Setup Utility

Choose which modules to modprobe (load) during boot. Some module(s) might
already be checked because they were modprobe'd or selected earlier.      ^(-)

[ ] Coda file system
[ ] SMB file system (Windows shares)
[ ] NCP file system (NetWare volumes)

<- Exit and save
<- Exit without saving
```

replimenu 0.7 (c) 2003 Michel Blomgren

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.

SENTINIX Setup Utility

Here you may configure your network interface(s), host and domain name, name servers and default gateway address. If you want to use a DHCP server for any interface, write "dhcp" into the "IP address"-field instead of an IP address.

1. Specify your fully qualified domain name (e.g. server1.sentinux.org)
2. Specify default gateway IP
3. Name server 1 (DNS)
4. Name server 2 (DNS)

Configure IP and netmask for your Ethernet device(s) below.

- + Enter IP address for eth0
- + Enter netmask for eth0

- <- Save and exit
- <- Exit without saving

replimenu 0.7 (c) 2003 Michel Blomgren

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.

SENTINIX Setup Utility

Choose which services to load at boot-time.

- SSH daemon
- FTP server (pure-ftpd)
- Postfix SMTP server
- Apache web server
- MySQL Database server
- Nagios Network Monitor
- Nessus Security Scanner
- Snort Network Intrusion Detection System
- Cacti - RRDTool graphing interface
- SNMP daemon
- NTP daemon

- Run MailScanner+SpamAssassin with Postfix?

- <- OK, I'm done

replimenu 0.7 (c) 2003 Michel Blomgren

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 "sentinux." You may use options 8 to reset your root password.
33. Select "Quit" to exit the setup program and return to the installation program.

SENTINIX Installation Procedure

Welcome to the installation process of SENTINIX.

Move up and down the menu using the arrow keys, PGUP/PGDOWN and HOME/END. Select an item by pressing return. If you want a console, press Alt+F2, Alt+F3, etc. You may quit by pressing F10 or "Q".

1. Choose your keyboard map
2. Start the installation process

-> Reboot the system

SENTINIX (C) 2003 Michel Blomgren. Built using the GNU/Linux system and other Open Source software. Linux is a trademark of Linus Torvalds. BusyBox (C) Erik Andersen. openMosix (C) Moshe Bar.

replimenu 0.7 (c) 2003 Michel Blomgren

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.

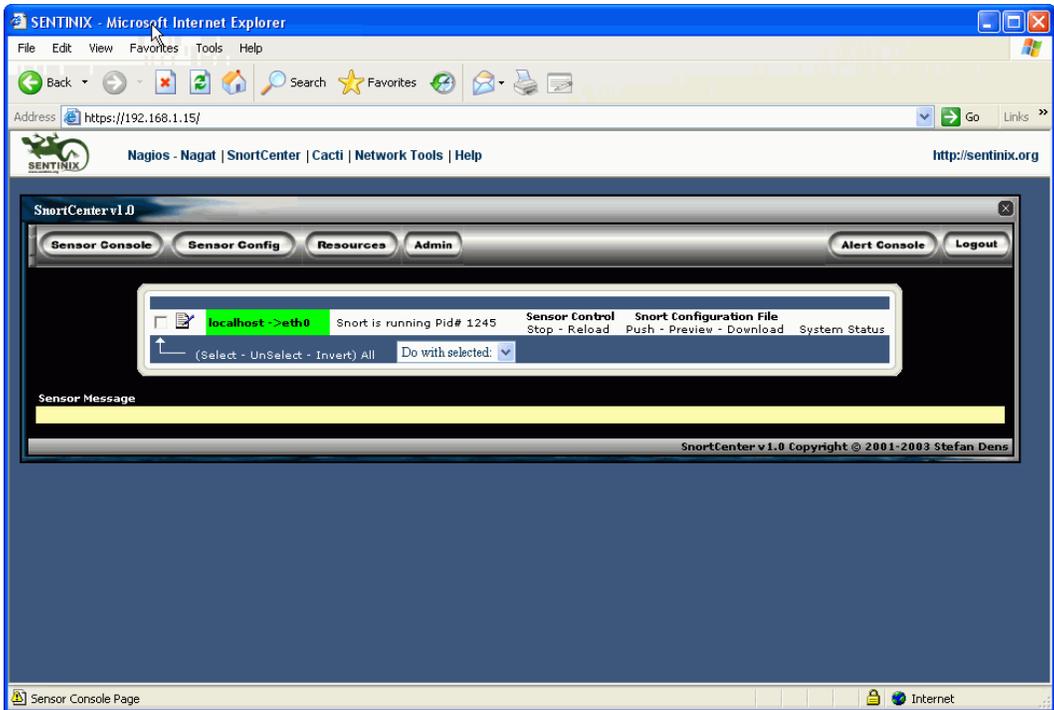


Figure 2 - SnortCenter Console

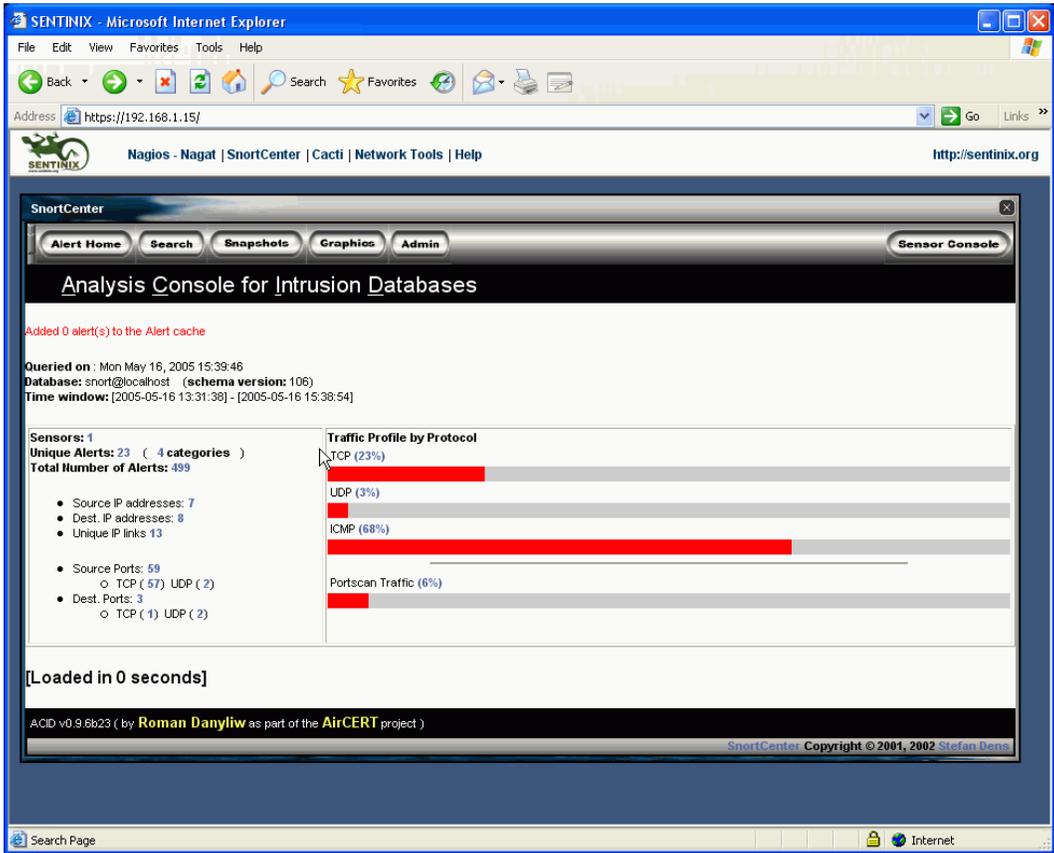


Figure 3 - ACID Summary Page

< Signature >	< Classification >	< Total Sensor # >	< Src. # >	< Dest. Addr. >	< Dest. Addr. >	< First >	< Last >
<input type="checkbox"/> [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
<input type="checkbox"/> arachnids[snort] ICMP L3retriever Ping	attempted-recon	51 (10%)	1	3	3	2005-05-16 13:32:11	2005-05-16 15:37:50
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> arachnids[snort] ICMP PING NMAP	attempted-recon	3 (1%)	1	2	1	2005-05-16 13:33:29	2005-05-16 15:07:29
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> [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
<input type="checkbox"/> 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
<input type="checkbox"/> [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

Action

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