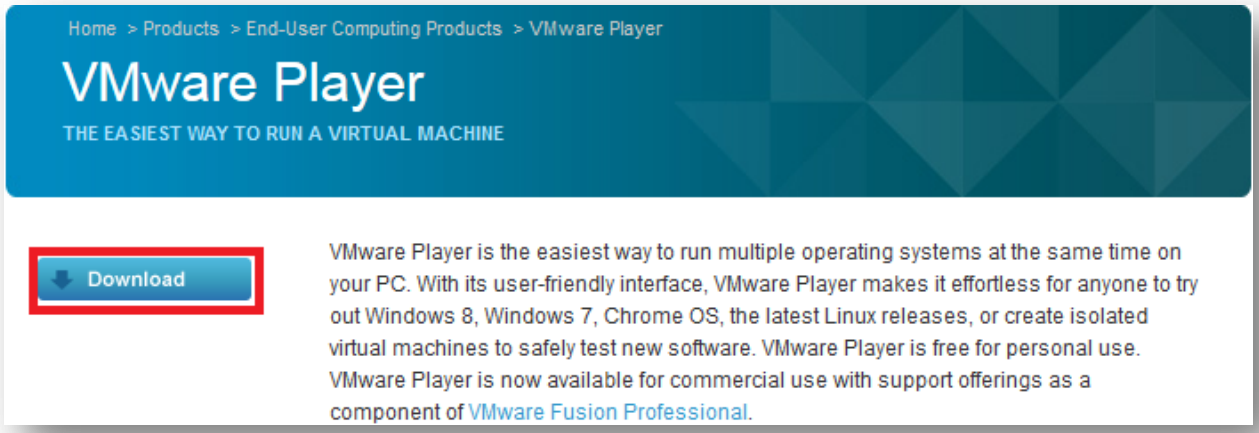
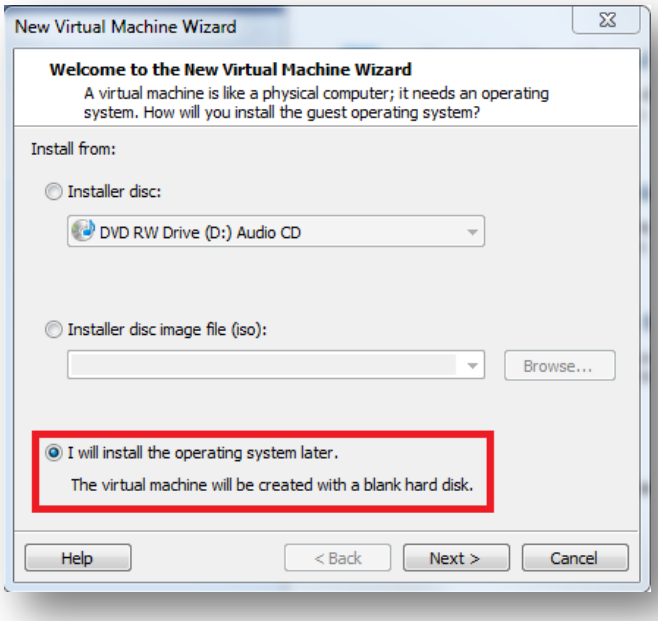
Guidance: Installing Autosnort via VMware Player.

The purpose of this document is to guide Autosnort users on how to install Autosnort on a Linux platform of their choice on VMware Player with a Windows Operating system as the host operating system.

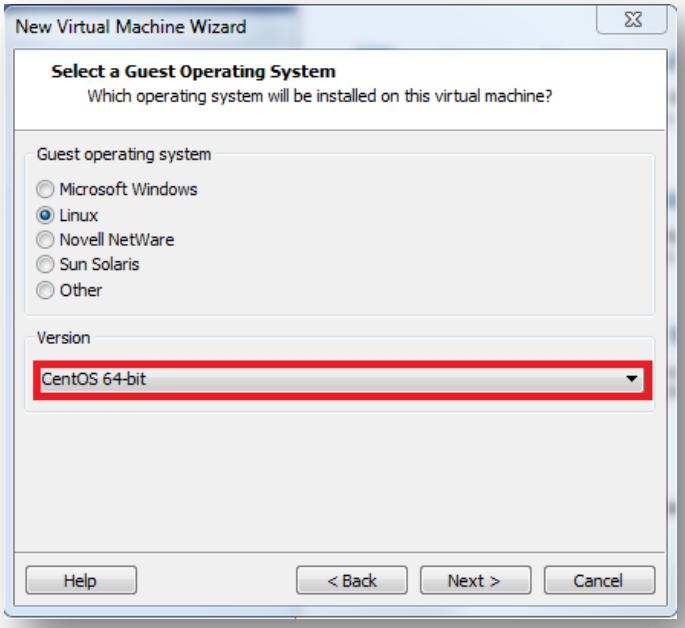
1. Download and Install VMware Player via vmware.com



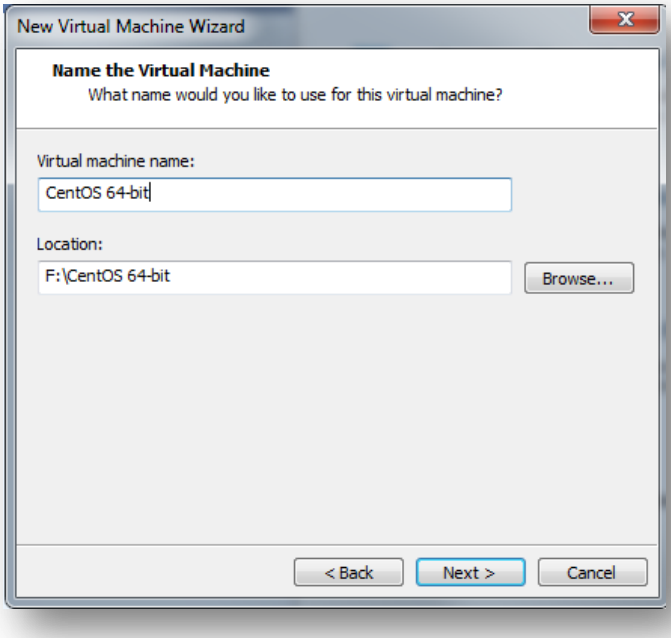
2. Download a Linux ISO for an Autosnort-support operating system. Choices include:
    a. CentOS (6.x)
    b. Debian (6.x)
    c. Ubuntu (12.04+)
    d. Backtrack (5r3, with Kali support coming soon!)
        i. For this document we will be using CentOS as the guest virtual machine operating system.
3. Run the New Virtual Machine wizard. Do not choose to install via CD or the .iso install method; choose “I will install the OS later.” The reason for this is that the “Easy Install” option makes a lot of assumptions that we do not want it to make.

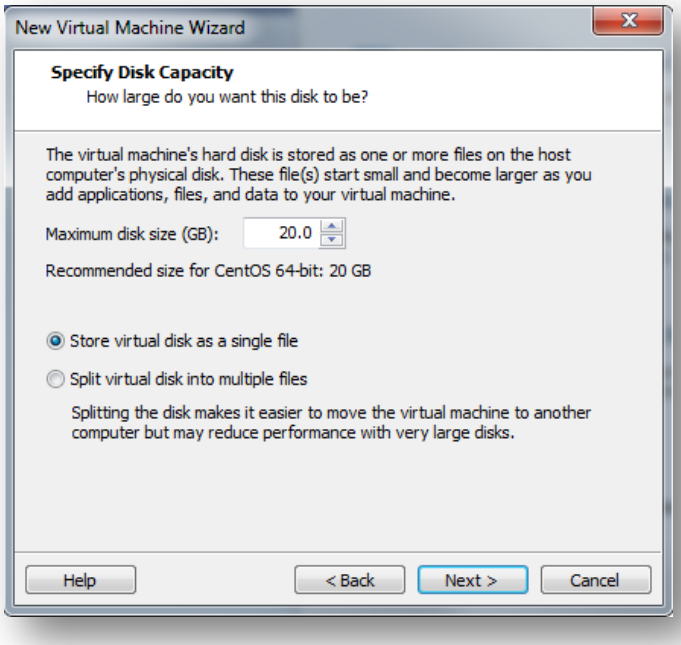


4. On the next page, choose CentOS or CentOS 64 bit.
    a. If you are installing another supported operating system, try these options:
        i. For Ubuntu, obviously choose Ubuntu or Ubuntu 64 bit
        ii. For Debian, choose Debian 6 or Debian 6 64 bit.
        iii. For Backtrack Linux, choose Ubuntu or Ubuntu 64-bit (BT is Ubuntu derived)

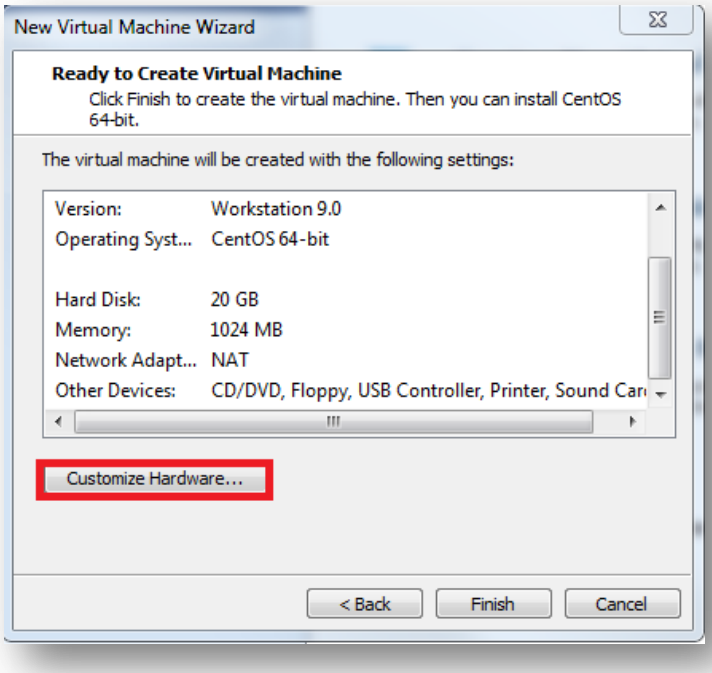


5. For the next two options, Choose to store the virtual machine file wherever you see fit. The default VM disk size for my CentOS 64-bit install was set to 20gb, this is a fairly good estimate and should more than serve you well. I choose to store the virtual machine as a single file.



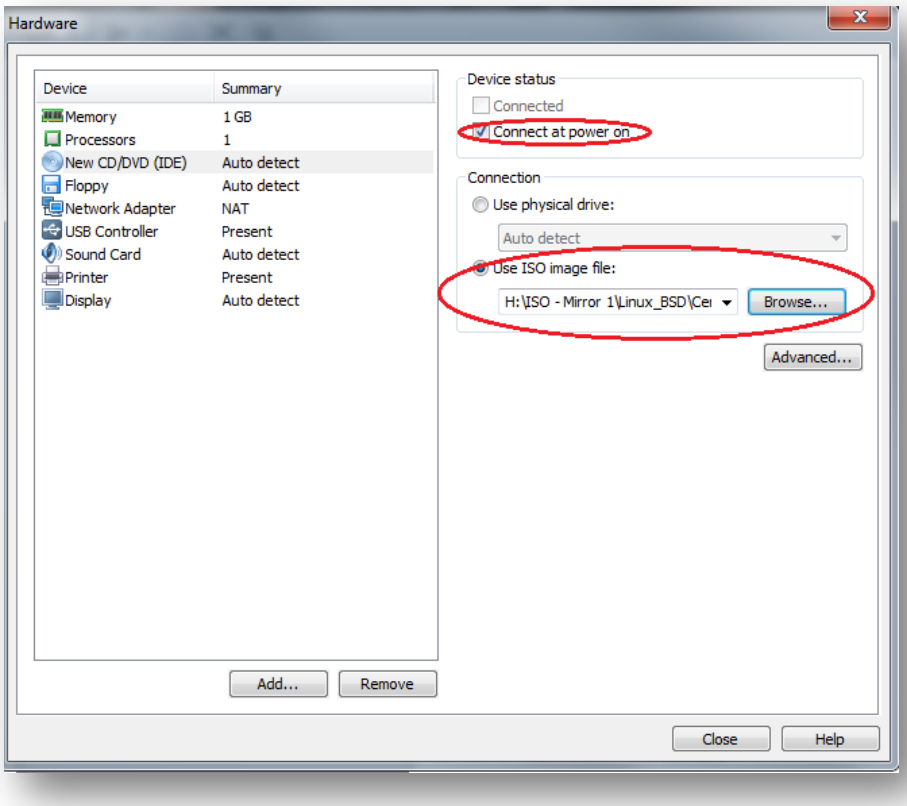


6. The final page will have you confirm your settings. We're not quite done here yet however; choose the "Customize Hardware" option, because we have some changes to make..

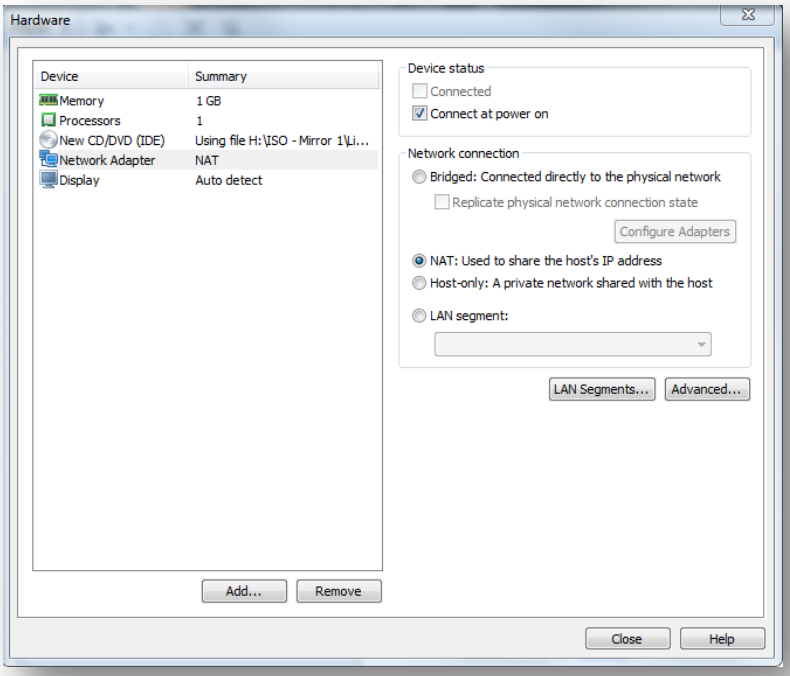


7. Here is where the fun begins. This page shows you all of the default hardware installed with your vm. The first change we need to make is to the New CD/DVD (IDE) option. Remember when we skipped having VMware do the "Easy Install" option? We now have to point the Virtual Machine to its installation ISO; this is the equivalent of taking a newly built computer and giving

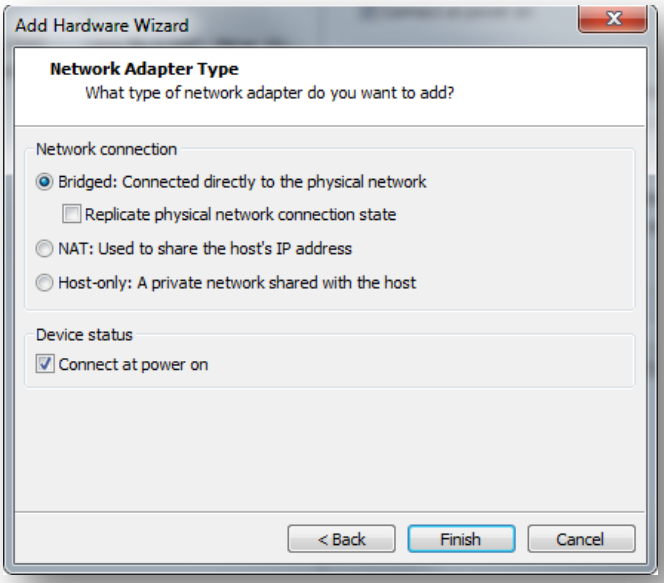
it a CD to boot off of to install its operating system. Click on New CD/DVD and choose “Use ISO image file:” and click browse. Point VMware to the the .iso file you downloaded. Make absolutely sure the “Connected at power on” option is checked on. Your screen should look something like this:



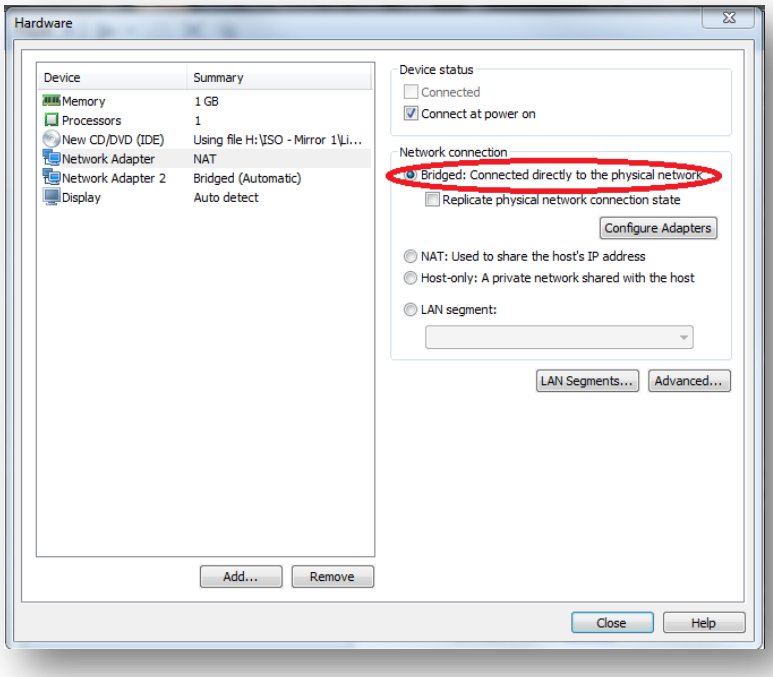
8. I would recommend removing the Printer, Sound Card, USB Controller, and Floppy options by selecting each piece of hardware and click the remove button at the bottom of the window; You won't need any of those features, so you may as well remove them to streamline the VM and reduce possible attack surface. As far as memory goes, the default 1GB should be fine. I would recommend using no less than 512mb for the VM. The hardware window should look something like this at this point:



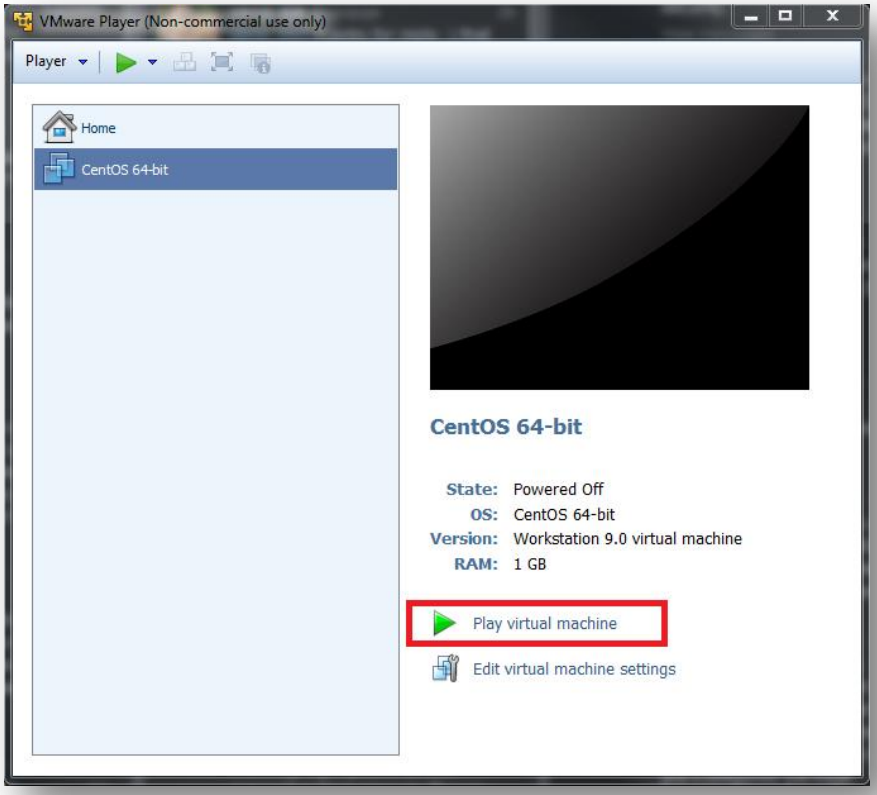
9. Next, You'll want to select the add button at the bottom of the window; we want to add a new network card. Most IDS/IPS systems should have a minimum of two network interfaces. One to carry service and maintenance traffic, and the other dedicated solely to sniffing network traffic. Your. Select "Add…" and choose "Network Adapter" then click Next. On the next window, you will be asked to choose the Network Adapter Type. Really this page is asking you what virtual network you want to plug the virtual network adapter to. Choose Bridged, and the "Connect at power on" option. Click Finish. The window should look something like this:



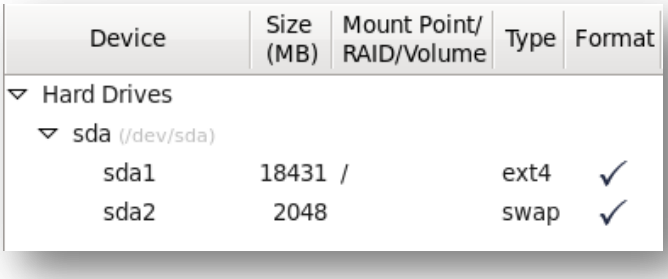
10. You should now have two Network Adapters – Network Adapter, and Network Adapter 2. Modify Network Adapter to use the Bridged Setting as well:



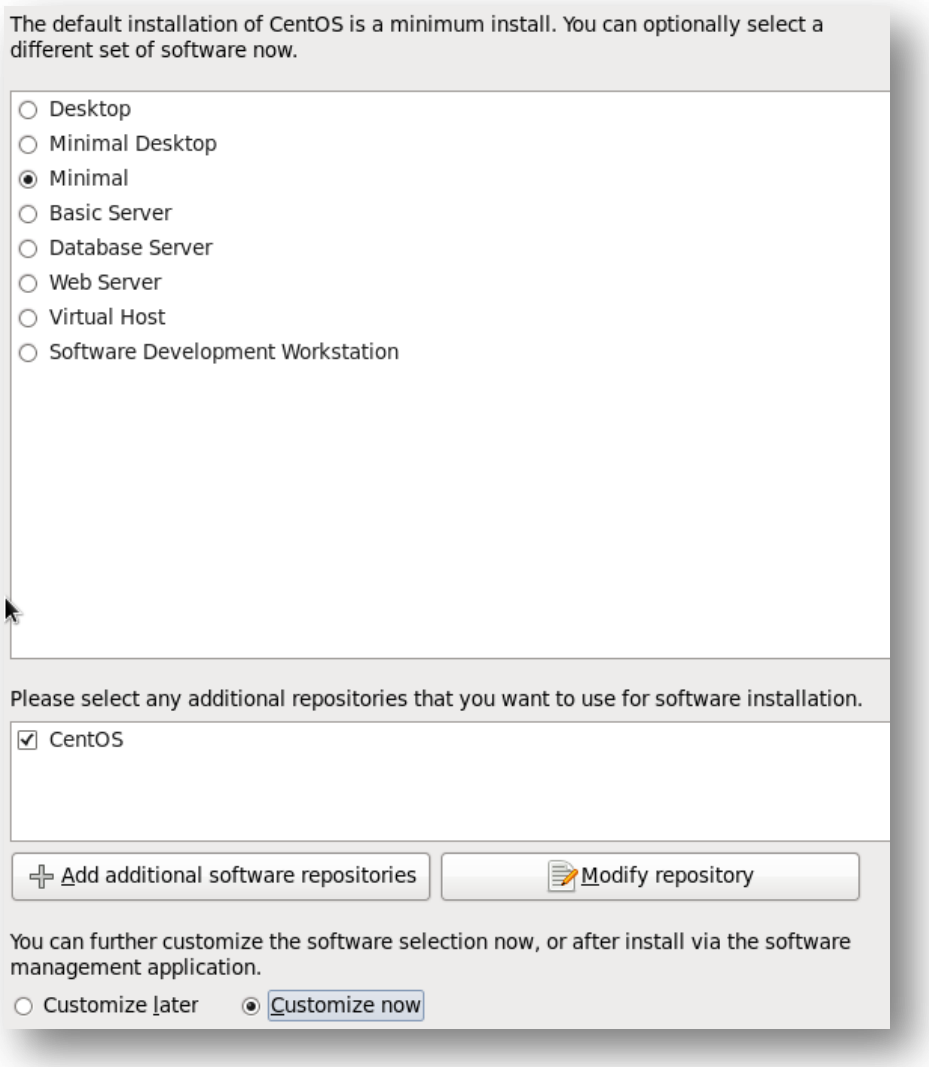
11. At this point, Select “Close” on the Hardware menu, and Click Finish on the New Virtual Machine Wizard. VMware Player should now have your new virtual machine in the menu. If for some reason you missed installing the second network card or reconfiguring the network cards, you may select the virtual machine and select “Edit virtual machine settings” if you need to make changes. For now, click play virtual machine. To turn on the Virtual Machine and begin the OS installation process.



12. You may be asked to install vmware tools. This choice is entirely up to you. I chose not to and continued the OS install. I will usually run through the defaults of a CentOS installation until I reach the partition manager. I don’t particularly care for LVM or mdadm or any of that fancy stuff since this is just a linux vm on another host OS. I’ll usually create a single swap partition twice the size of ram, and give the rest of the disk to a “/” partition and go about my business.



13. After creating the partitions and installing the boot loader (I use default settings), I move on to the package installation partition. Usually I will go with a minimal installation and choose the "Customize Now" option on the bottom of window:



14. Select Next. Select the option "Base System" and check the Base option with a cog next to it:

15. Click the "Optional Packages" option at the bottom of the screen. Here are packages I would recommend uninstalling:
    a. Acpid
    b. B43-fwcutter
    c. Dmraid

d. Dosfstools
e. Eject
f. Fprintd-pam
g. Hunspell
h. Hunspell-en
i. Ledmon
j. Lvm2
k. Mdadm
l. Pcmciautils
m. Pinfo
n. Pm-utils
o. Plymouth
p. Rdate
q. Rsync
r. Smartmontools
s. Usbutils
t. Virt-what
u. Wireless-tools
v. Words
w. Xz
    i. After unselecting these packages you should be sitting at 51 out of 116 packages in the base installation package. Afterwards, click next (Unless there are extra things you would like to install. This is all I usually install)

16. The installer will resolve your dependencies. I only had 316 packages in total to install ☺

17. After the packages install, let the installer reboot your vm.

18. I would recommend making the following change to eth0:
    a. Vi /etc/sysconfig/network-scripts/ifcfg-eth0:
    b. Mofidy this file to have these settings:

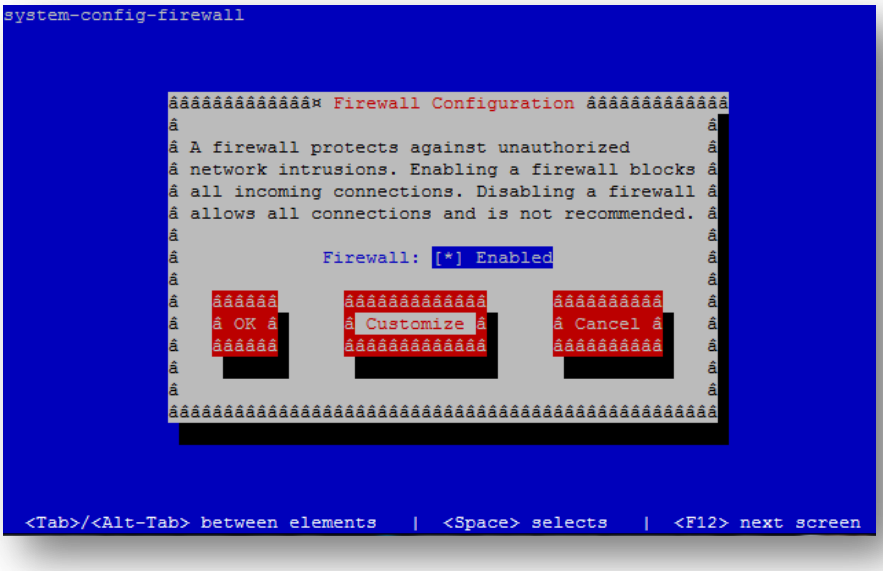
```
DEVICE="eth0"
BOOTPROTO="dhcp"
HWADDR=[default MAC address]
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
UUID=[default UUID]
```

19. I would also advise configuring /etc/sysconfig/network-scripts/ifcfg-eth1 and changing NM_CONRTROLLED to “no”, ONBOOT to “yes” and BOOTPROTO to “static”. This enables eth1 to be up on boot, with no ip address and ready to sniff traffic (aka ready to serve as our sniffing interface)

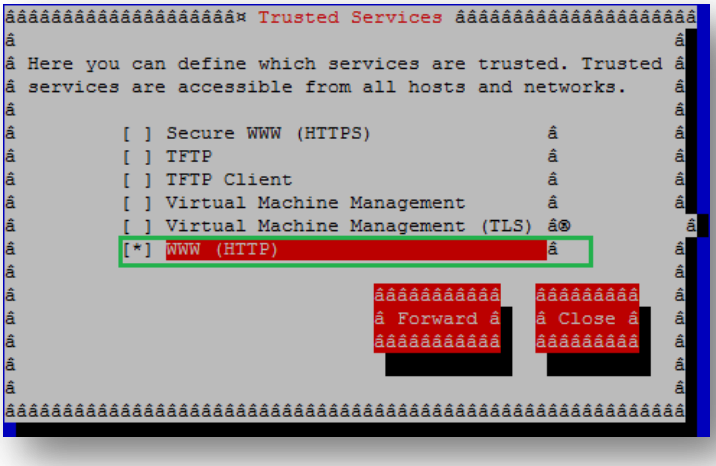
20. Next, run “dhclient eth0” to give your eth0 address an ip address via your network’s DHCP server. Afterwards, run ifconfig eth0 to get your dhcp assigned address. You should now be able

to use an ssh client to manage your CentOS vm; CentOS usually installs sshd and makes a firewall rule to allow sshd by default.

21. Next, run “system-config-firewall-tui”. Hit tab or the down arrow until “Customize” is highlighted and hit enter. Your screen will look something like this if you are running the tool over putty, like I am:



22. Hit the down arrow to go all the way to the bottom until WWW (HTTP) is highlighted. Hit the space bar and an asterisk should appear in the “[ ]” box next to it Next, hit tab twice to select close and hit enter :

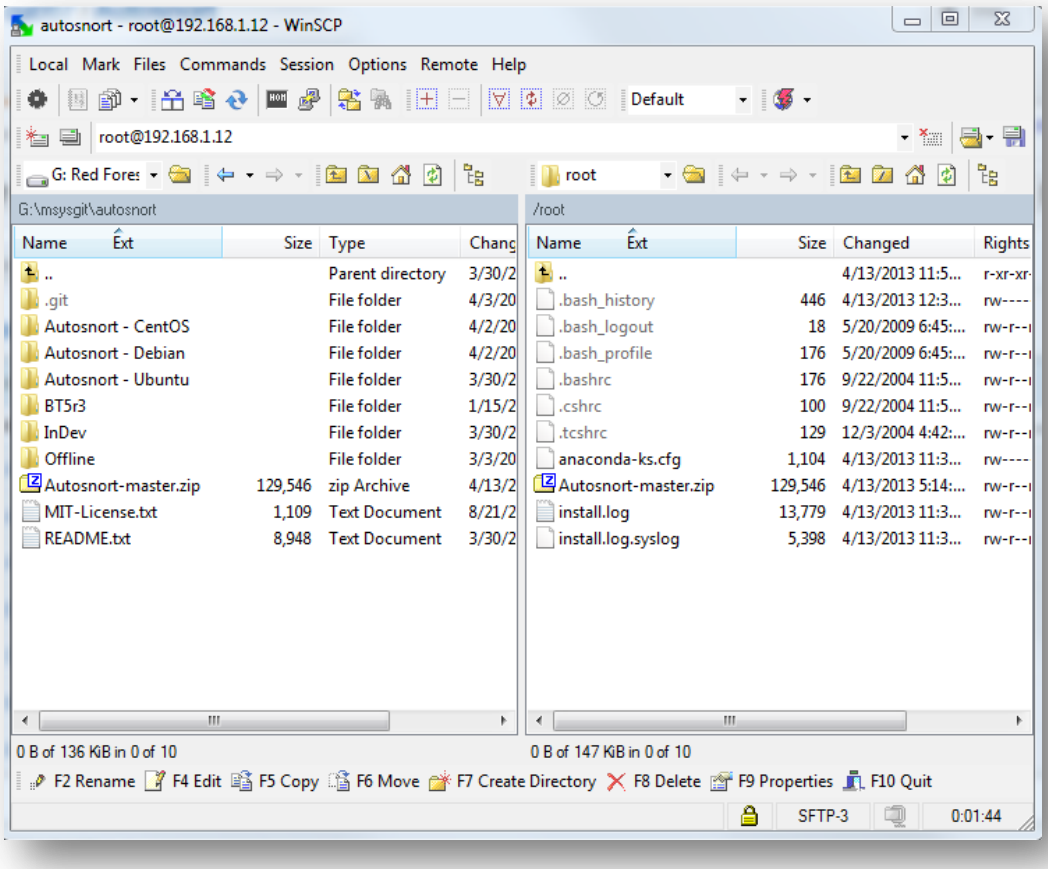


23. Click ok to exit, then select yes to be dropped back into your regular shell.
24. At this point, you may wish to test to see what traffic eth1 will be able to pick up from the bridge mode networking. Try running “tcpdump –i eth1 not port 22”. This will allow you to see

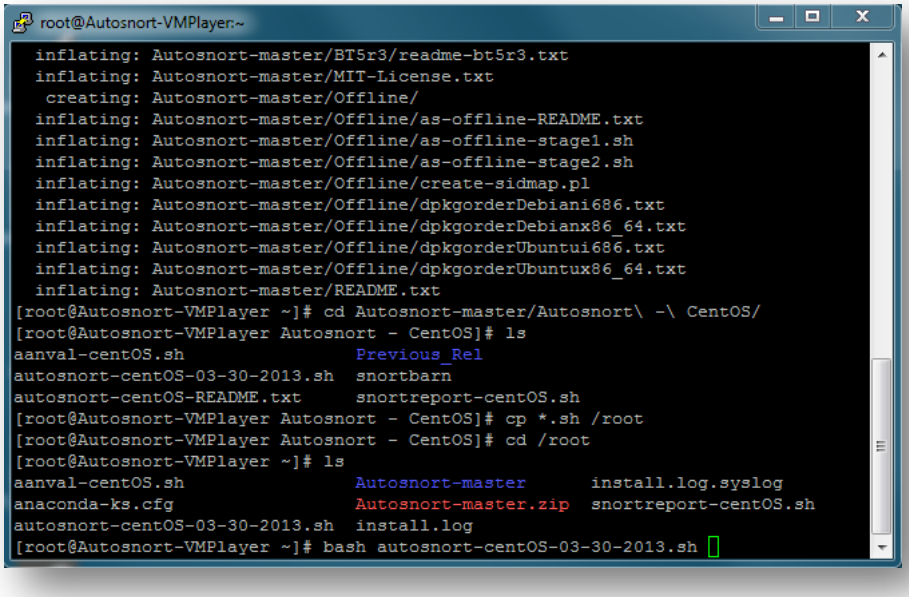
what traffic your eth1 adapter on the virtual machine will see. On most home networks and corporate networks, you will likely be connected to a switch or a broadband router. In these cases you will only be able to see traffic coming to/from the sensor and to/from the host operating system. There are special things you can do to change this that require extra hardware and hacking know-how, but for now let's start this off easy. Run the command above. If your host OS is busy (e.g. you have a web browser up browsing the web, or twitter or some other applications that talk over the internet) you should be seeing all sorts of traffic. If you aren't seeing a lot of traffic try opening up a command prompt and pinging google.com. If you are able to see the pings to and from your host operating system, you should be all set!

25. Visit the Autosnort github page and download the entire script archive as a .zip. or alternatively you can install git on to your centOS vm and just pull the repository down via the git protocol.

    a. If you chose to download the github repo as a .zip, use an scp client (WinSCP for windows is excellent) and use that to upload the .zip to your guest operating system:



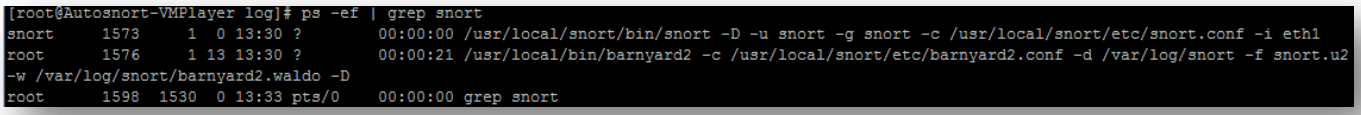
26. Run the unzip command on the Autosnort-master.zip file. Next, cd into "Autosnort-master/Autosnort\ -\ CentOS/" and run the command "cp *.sh /root" to copy all the relevant shell scripts to /root.
27. Finally, run Autosnort: "bash Autosnort-centOS-[date stamp].sh:



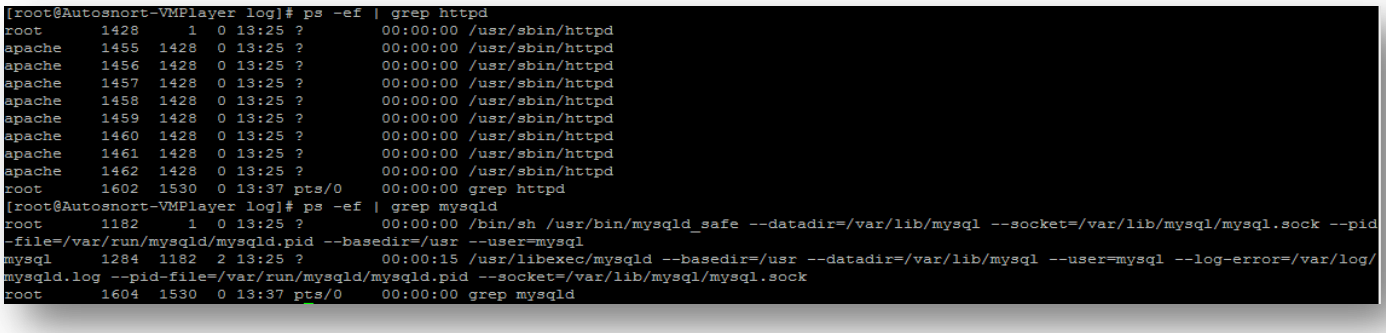
28. At this point, run through the Autosnort installation script. The script will prompt you for the information it needs when it needs it:
    a. You will be prompted to enter a new mysql root user password
    b. You will be prompted to enter a new snort user account password
    c. You will be prompted to choose the method you wish to use to install snort rules
        i. Via PulledPork (HIGHLY recommended)
            1. If this method is chosen, you must supply the script with a snort.org oinkcode, and choose whether or not to download rules for the current snort release or the previous release of snort (if you do not have a VRT subscription, and the newest version of snort is less than 30 days old, you must install rules from the older snort release)
        ii. Via VRT rule tarball
            1. If this method is chosen, you need to supply the path and the name of the VRT rule tarball you wish to use.
    d. You will be prompted to enter a password for the snort mysql (database) user
        i. It is very important you remember this password.
            1. It will be used by barnyard 2 to import events into the snort intrusion event database
            2. used by snortreport to read events from the database and display them on the web UI
            3. used by Aanval to import events from the snort database to the aanval database used by their product.
    e. You will prompted to enter the mysql root user password at least 3 times
        i. Once to create the snort database for barnyard2
        ii. Again to create the snort database schema for barnyard2
        iii. Again to create the snort database user barnyard2, snortreport and/or aanval all use for event update/access

f. You will be prompted to choose the interface you want snort to sniff traffic on
g. You will be prompted to decide if you want snort and barnyard2 to be started on system boot via rc.local entries
h. You will be prompted to choose what UI you wish to install to review snort intrusion events (current choices are snort report or Aanval)
    i. If installing snort report on Debian or CentOS you will be prompted if you wish to install fixes required for snortreport to properly display events on either of these operating systems
    ii. If installing aanval on any operating system you will be prompted to enter the mysql root database user twice – once to create aanvaldb and again to grant the snort database user the ability to modify the database. The snort database user and password should be entered when installing aanval when it asks for the username and password that will be used to maintain the aanvaldb.
i. You will be prompted one last time to reboot the system.

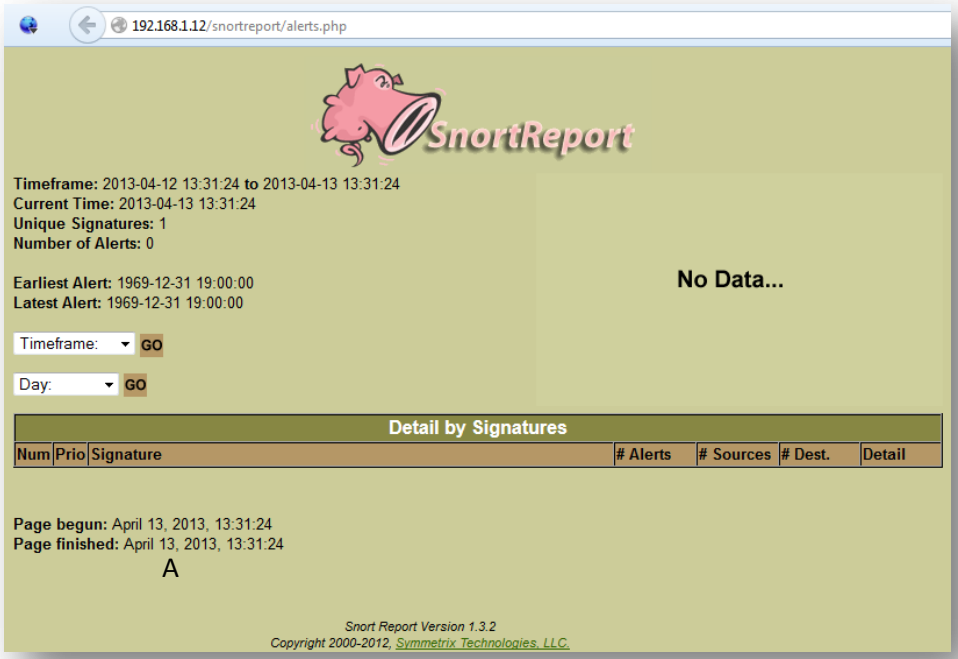
29. Allow the virtual machine to reboot and log back in. Run the follow commands:
    a. Ps –ef | grep snort – you should have these entries:



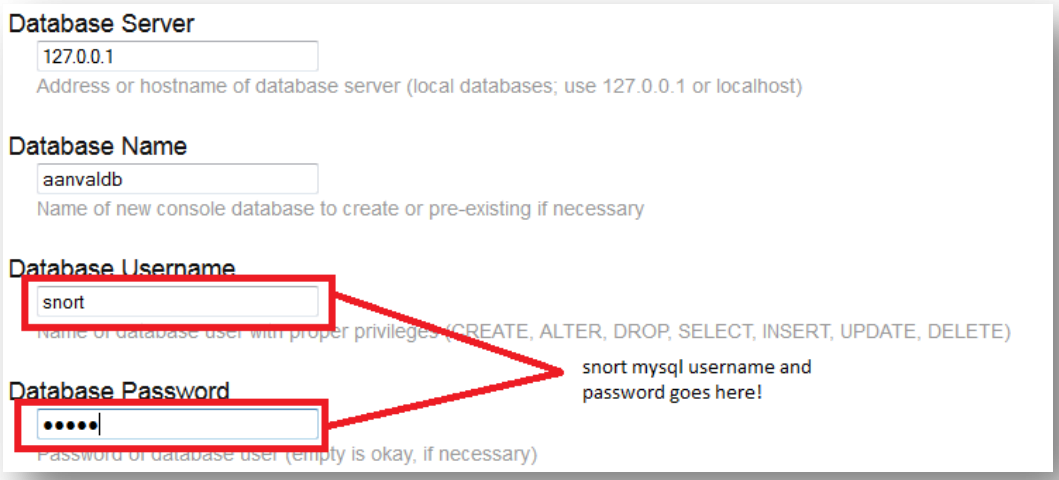
    b. ps –ef | grep httpd (or on Ubuntu/Backtrack/Debian, ps –ef | grep apache), and ps –ef | grep mysqld:



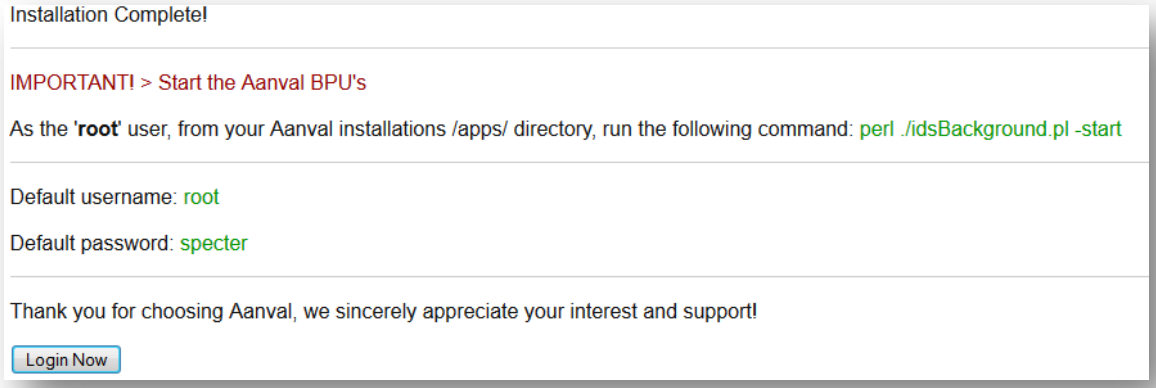
30. Try logging into the web interface you choose to install.
    a. If you choose to install snortreport navigate to: http://[eth0 ip address]/snortreport:



b. If you have any alerts, at this point, they should begin to show up here.
c. If you opted to install aanval, navigate to http://[eth0 ip]/aanval
    i. You will be run through a guided install upon your first visit to the aanval console. On the third page you will be asked to input information for the web console to access the aanvaldb. Input the following:

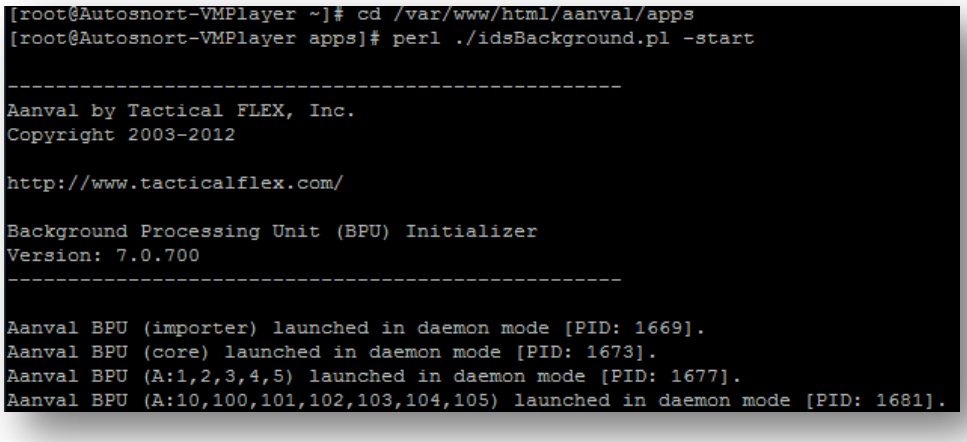


d. The next page will indicate you need to start the aanval BPUs and grant you the aanval console default login credentials (root/specter):



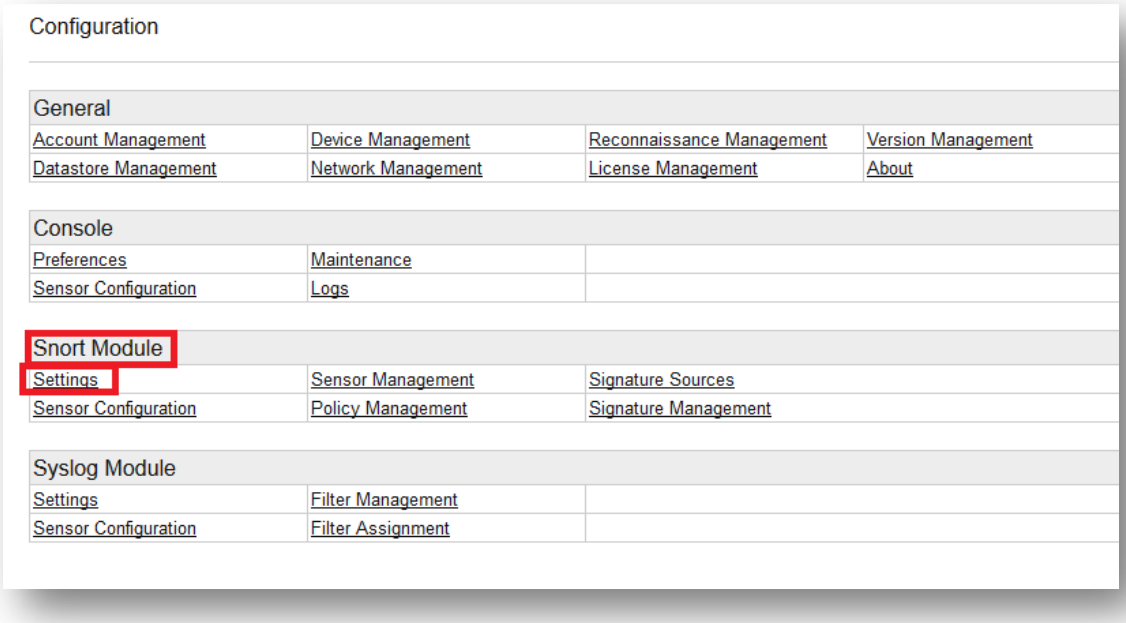
e. The idsBackground.pl script is located in the 'apps' directory under the 'aanval' directory under the webroot directory for your linux distribution.
   i. For Ubuntu and Debian, this should be /var/www/aanval/apps
   ii. For Redhat/CentOS this should be /var/www/html/aanval/apps

f. Cd to the apps directory and run "perl ./idsBackground.pl –start" to start the BPUs. The BPUs are responsible for importing data from the snort database that barnyard2 imports data to, and transferring it the the aanvaldb that aanval uses.
   i. **The BPUs must be started for aanval to update the intrusion events the console displays. This means that if your sensor restarts or reboots for any reason, you will need to manually restart the BPUs, or implement an init script or an entry in rc.local to do this automatically!**

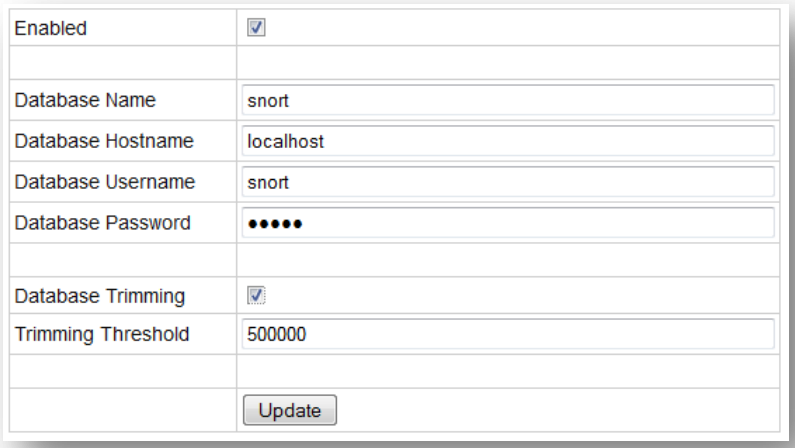


g. Upon logging into the aanval console, click the gear symbol in the lower right hand corner:

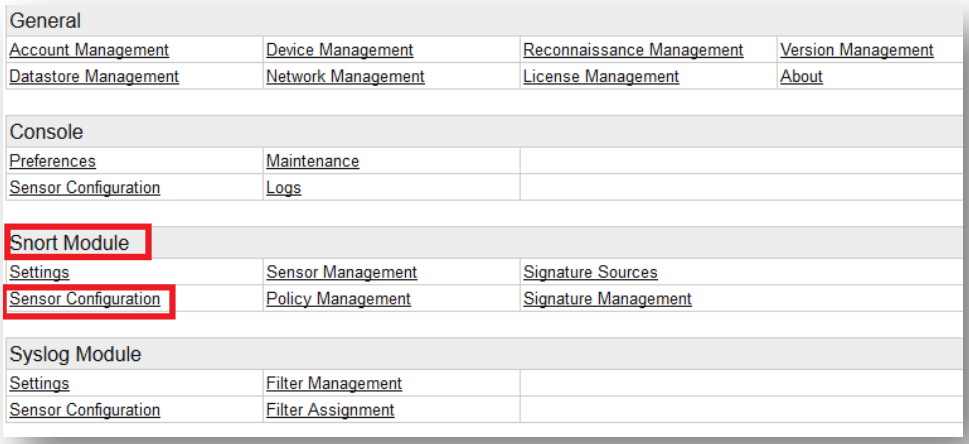
h. This will bring you to the Configuration page. Click “Settings” under “Snort Module”:



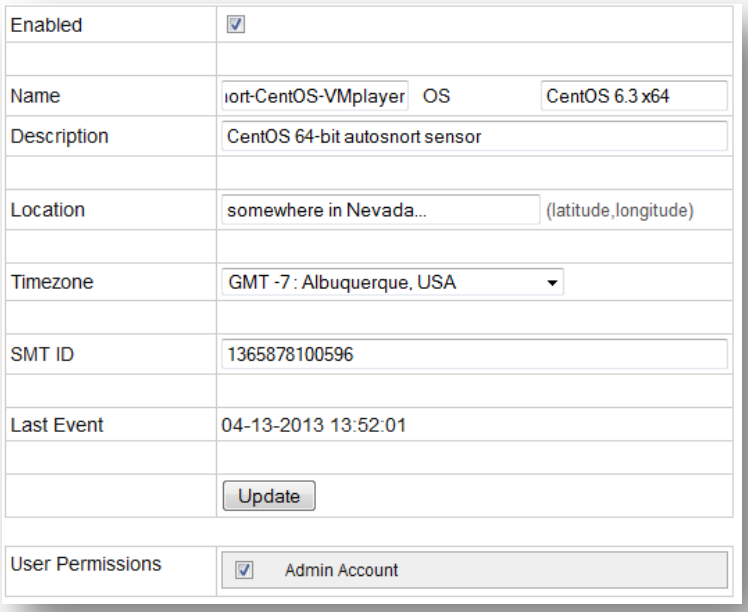
i. On the next page, you will want to enable the snort module and input the configuration settings used for the snort database that barnyard2 dumps intrusion events to.
    i. The database name is ‘snort’
    ii. The database host is ‘localhost’
    iii. The database user is ‘snort’
    iv. The database password is the password for the snort database user.
    v. For this installation, I chose to enable database trimming.
        1. For home users, there is near to no harm in enabling this; it essentially clears the oldest events from the snort database after the database of events hits a certain threshold.
        2. For corporate or professional users, please consult your data retention policies and data backup procedures before enabling this feature.
    vi. Click update. The page should look something like this before updating your settings:



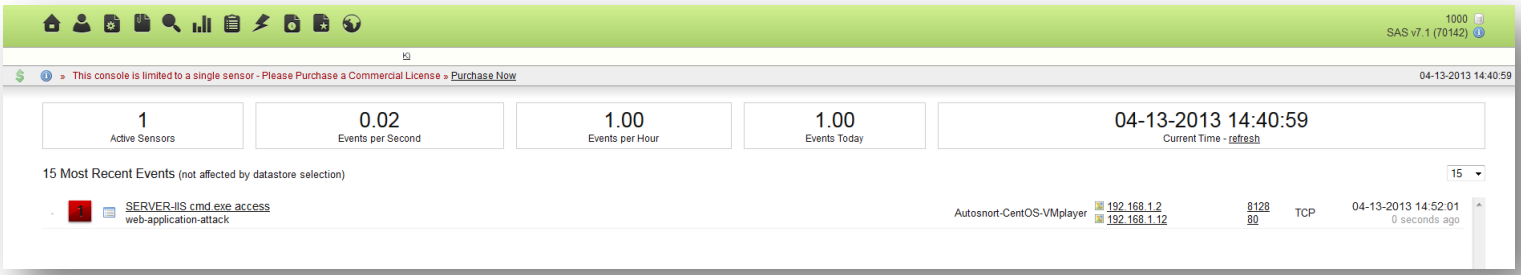
j. After clicking update, go back to the Configuration page by clicking the gear symbol again, and select “Sensor Configuration”:



k. On this page, click enabled, and the select update; this must be done to modify the user permissions field. After hitting update, check “admin account” under user permissions. Fill out the remaining fields As befitting for your sensor installation:



31. At this point, the installation should be completely finished. Click the symbol that looks like a house in the upper left hand corner of the page to go back to the home page. If snort recorded any alerts, you should see events here.



Special tactics and techniques: how to get your vmware player virtual machine to see more than just what the host OS sees

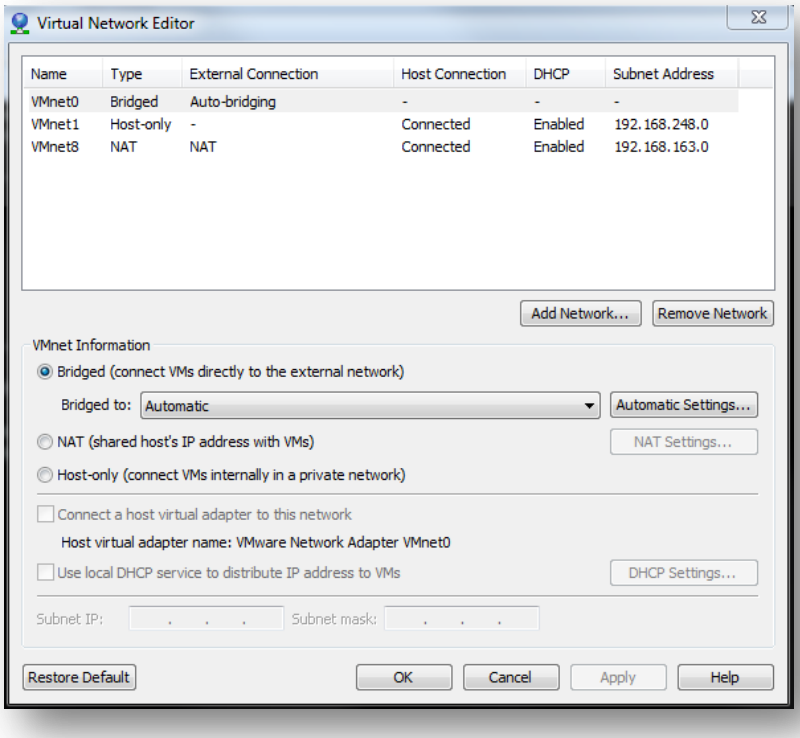
This is a special guide on how to get a vmware player installation of Autosnort to see more than just traffic to the sensor itself and the host operating system.

Recall above how this is a network based limitation. Before attempting this you will need the following:

- A Host Computer with at least two physical network interface cards

- A switch capable of spanning network traffic, or a network tap to feed traffic to your virtual machine from other network nodes you want to monitor
- A copy of vmware workstation 9 (or whatever the latest edition is) downloaded via vmware.com
    - A copy of vmware workstation can be downloaded for free. Do not worry about the licensing, we're only going to install it for 5 minutes at most, then uninstall it immediately.
- A good text editor (if on windows, recommend using notepad++ for this)

1. Download vmware workstation via vmware.com and install it.
    a. If you have already install vmware player, it will automatically uninstall it and then install vmware workstation. Don't worry! Your virtual machine is still here.
2. Run through the entire installation. When it prompts you for your product key, click skip. We won't be using the software at all, so don't worry.
3. After the installation is done, you will want to navigate to the program files directory you installed vmware workstation in – by default this is C:\Program Files\VMware\Vmware Workstation
4. In this directory, locate the file "vmnetcfg.exe" It will have a globe with a green line below it as its icon, and be approximately 4.73MB in size. Copy the file to another location; like your desktop.
5. Uninstall vmware workstation; we got what we wanted.
6. Install, or re-install vmware player.
7. Copy the vmnetcfg.exe file to the installation directory for vmware player – usually C:\Program Files\VMware\VMware Player
8. Create a shortcut to vmnetcfg.exe to your desktop and double click it. If everything was successful, you'll end up with this:

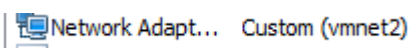


9. Click Add Network and add another virtual network. For your new virtual network, make it a bridged network. I chose vmnet2 as the vmnet to use.
10. Under the bridged settings, bridge it to the network interface you are plugging the span or tap port into.
11. Under the original bridge net, vmnet0, under the bridged setting changed 'bridged to:' from automatic, to the the interface you will use to connect the sensor's eth0/management interface to the network for updates and managed via http/ssh. Select ok to close.
12. Next, we have to find our virtual machine's vmx file. When you initially configure the virtual machine via vmware player's wizard you have to give the virtual machine a home directory. For example, mine was F:\CentOS 64 bit
13. In this directory you will to save a copy of the virtual machine's .vmx file (just in case) and edit the .vmx file. There should be multiple ethernet0 and ethernet1 entries in this file. These are bits of metadata that control how the virtual network adapters work on the virtual machine. The "edit virtual machine settings" won't let us connect to the vmnet2 that vmnetcfg.exe let us create, but adding the entries into the virtual machine's .vmx file will let us do this.
14. Find the entries for your sniffing interface. Let's choose ethernet1 as our example. You should have a group of entries that look like this:
    ethernet1.present = "TRUE"
    ethernet1.virtualDev = "e1000"
    ethernet1.wakeOnPcktRcv = "FALSE"
    ethernet1.addressType = "generated"

    Add these entries to that:
    ethernet0.connectionType = "custom"
    ethernet0.vnet = "vmnet5"

    This should be the end result:
    ethernet1.present = "TRUE"
    ethernet0.connectionType = "custom"
    ethernet0.vnet = "vmnet2"
    ethernet1.virtualDev = "e1000"
    ethernet1.wakeOnPcktRcv = "FALSE"
    ethernet1.addressType = "generated"

    Save your .vmx file and open vmware player. Select 'edit virtual machine settings' If you see this under your second virtual network adapter, you know your configuration changes were successful:

15. Power on your vm, login and run "tcpdump –i eth1 not port 22" and see if you can sniff traffic from other systems via your span or tap.

Special Tactics and Techniques: Installing the snortbarn init script on CentOS/Redhat for better service management and removing the rc.local entries

This guide will show you how to replace the rc.local entries Autosnort creates for snort and barnyard 2 and replacing them with a traditional init script. To do this, you will need:

- The Autosnort github .zip file or github repo on the target virtual machine/sensor you want to install the init script to

If you've already installed Autosnort, the github repo or zip file should already be on your system, and so should the init script.

1. Cd to "Autosnort-master/Autosnort\ -\ CentOS/" and run "cp snortbarn /root" then "cd /root"
2. Run vi snortbarn to open the file up in the vi text editor

```
[root@Autosnort-VMPlayer ~]# cd Autosnort-master/Autosnort\ -\ CentOS/
[root@Autosnort-VMPlayer Autosnort - CentOS]# ls
aanval-centOS.sh  autosnort-centOS-03-30-2013.sh  autosnort-centOS-README.txt  Previous_Rel  snortbarn  snortreport-centOS.sh
[root@Autosnort-VMPlayer Autosnort - CentOS]# cp snortbarn /root
[root@Autosnort-VMPlayer Autosnort - CentOS]# cd /root
[root@Autosnort-VMPlayer ~]# vi snortbarn
```

3. Review the follow section of the init script and verify everything matches your Autosnort installation. If you followed recommend settings, everything should match perfectly:

4. Next, run "ls –al /etc/rc.d/rc?.d/S*mysqld*" the purpose of this command is determine what

```
# Change these variables to suit your snort installation
#The location of the snort binary
SNORTD=/usr/local/snort/bin/snort
#The location of the barnyard2 binary
BY2D=/usr/local/bin/barnyard2
#The sniffing interface for snort
snort_iface=eth1
#Command line execution options for snort
OPTIONS="-D -u snort -g snort -c /usr/local/snort/etc/snort.conf -i $snort_iface"
#Command line execution options for barnyard 2
OPTIONS2="-c /usr/local/snort/etc/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -D"
```

run levels and what order the mysqld script starts up overall on that runlevel. If you followed the Autosnort install guidelines above, mysqld should be present in /etc/rc.d/rc3.d/S64mysqld as the only startup script for mysqld:

5. the first 8 lines of snortbarn indicate that its configured to start on runlevels 3 4 and 5 with a

```
[root@Autosnort-VMPlayer ~]# ls -al /etc/rc.d/rc?.d/S*mysqld*
lrwxrwxrwx. 1 root root 16 Apr 13 13:04 /etc/rc.d/rc3.d/S64mysqld -> ../init.d/mysqld
```

startup script value of 65. This is important because it means snort and barnyard 2 are correctly configured to start up AFTER mysqld starts up. Barnyard 2 depends on mysqld to be running before it is started up. If for some reason snortbarn is scheduled to start up BEFORE mysqld is scheduled to start up, edit the number in the red square below to have a HIGHER value than the mysqld script above:

```
[root@Autosnort-VMPlayer ~]# head -8 snortbarn
#!/bin/bash
#
# snortbarn - Starts up Snort and Barnyard2
# chkconfig: 345 65 25
# description: Snort is a Open Source Intrusion Detection System
# This service starts up the snort daemon. #
# processname: snort
# pidfile: /var/run/snort_eth*.pid
```

6. Run the command “chmod u+x snortbarn” then “cp snortbarn /etc/init.d/” then “chkconfig --add snortbarn” to have the init script added to runlevels 3,4 and 5.
7. Next, remove the Autosnort entries from /etc/rc.local. This should be all that is left in /etc/rc.local on a default CentOS install:

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
```

8. Next, run the commands “killall snort” and “killall barnyard2” to kill any remaining barnyard2 and snort processes. Then run the command “service snortbarn start”

```
[root@Autosnort-VMPlayer ~]# killall snort
[root@Autosnort-VMPlayer ~]# killall barnyard2
[root@Autosnort-VMPlayer ~]# service snortbarn start
Bringing up snort interface                                [  OK  ]
Starting snort: Spawning daemon child...
My daemon child 9468 lives...
Daemon parent exiting (0)
                                                           [  OK  ]
Starting barnyard2:                                        [  OK  ]
```

9. You can use the command “service snortbarn start” to start up snort and barnyard2. You can use “service snortbarn stop” to stop the snort and barnyard2 processes instantly, You can use service snortbarn status to check the pids for the snort and barnyard2 processes, and you can use “service snortbarn restart” to stop then start the snort and barnyard2 processes.

```
[root@Autosnort-VMPlayer ~]# service snortbarn start
Bringing up snort interface                                [  OK  ]
Starting snort: Spawning daemon child...
My daemon child 10223 lives...
Daemon parent exiting (0)
                                                           [  OK  ]
Starting barnyard2:                                        [  OK  ]
[root@Autosnort-VMPlayer ~]# service snortbarn status
snort (pid  10223) is running...
barnyard2 (pid  10246) is running...
[root@Autosnort-VMPlayer ~]# service snortbarn restart
Stopping snort:                                            [  OK  ]
Stopping barnyard2:                                        [  OK  ]
Bringing up snort interface                                [  OK  ]
Starting snort: Spawning daemon child...
My daemon child 10368 lives...
Daemon parent exiting (0)
                                                           [  OK  ]
Starting barnyard2:                                        [  OK  ]
[root@Autosnort-VMPlayer ~]# service snortbarn stop
Stopping snort:                                            [  OK  ]
Stopping barnyard2:                                        [  OK  ]
[root@Autosnort-VMPlayer ~]#
```