**Course Project**

**College of Engineering and Information Sciences**

**DeVry University**

**Course Number: SEC290**

**Module 2: Snort**

**Objectives**

In this module, we will set up a distributed Snort with clicks of the mouse, including the following.

* Installing Snort
* Testing Snort Rules
* Creating Custom Snort Rules
* Deploying Multiple Snort Sensors

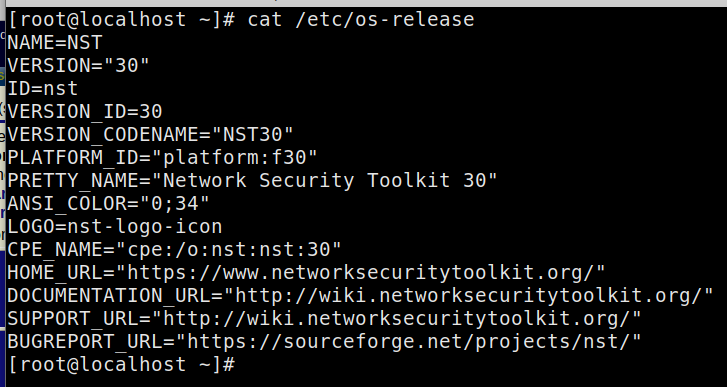
**Required VMs**

* Ubuntu-Web: username/password: **student/studentpassword**
* NST30: username/password: **root/rootpw**
* OWASP BWA Machine: username/password: **root/owaspbwa**

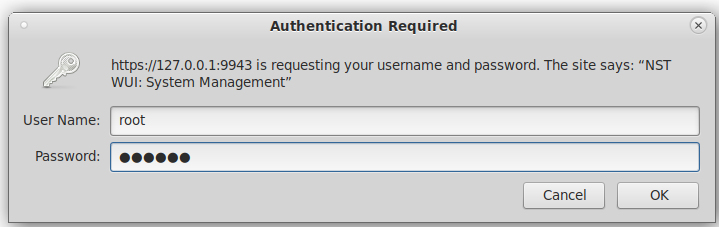
**Part 1: Installing Snort**

We are going to install Snort from the Linux machine Network Security Toolkit. In fact, the toolkit contains most of the top 125 free security tools with a web form front-end to make our work easier.

1. Power on the NST30 Machine and log in with the username/password **root/rootpw**. The Linux distro on this machine is Fedora. Click on the terminal icon at the top left and open a terminal window. Enter **cat /etc/os-release**.An example of the output is shown in the image below. We are using version 30 of the Network Security Toolkit.



1. To check IP configurations, enter **ifconfig** and notice thatFedora uses the **enp0s3** interface.
2. Click on **Applications | System Tools | NST Web Interface**. If prompted, enter the username and password (**root/rootpw**) as seen below.



1. Click on **Security | Intrusion Detection | Snort IDS – Sguil**.The output is shown in the image below.

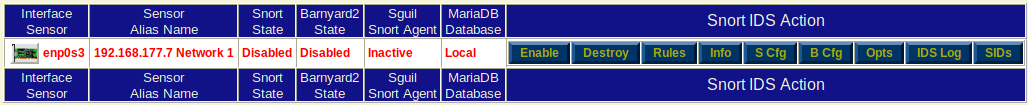




1. Select the interface radio button, scroll down, and click on **Setup**/**Start Snort** at the bottom of the screen as shown below.



1. Wait for the command to stop processing and click on **Check Status**. You will see the sensor details as shown in the image below.



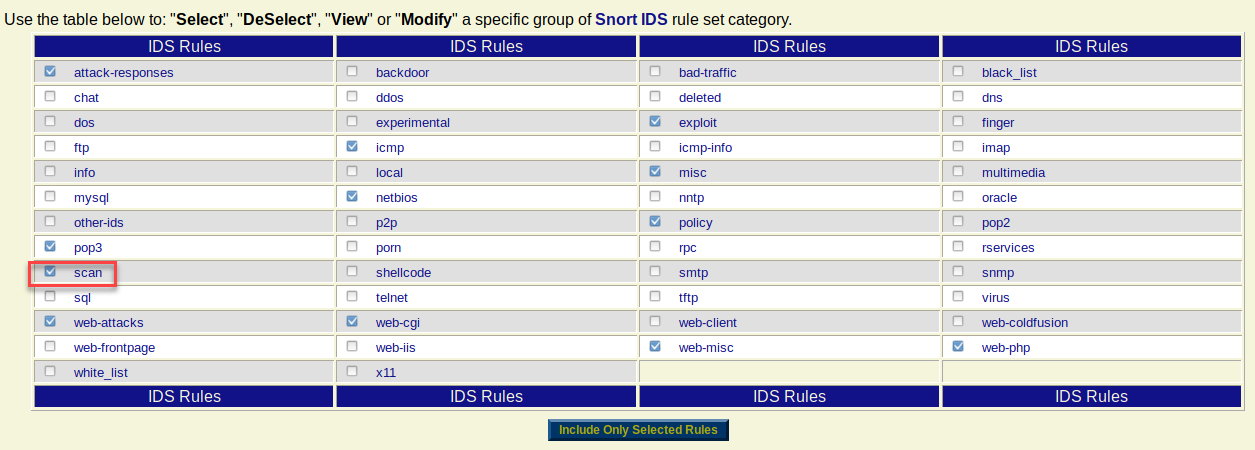
1. Click on the **Enable** button. Read through the messages of the startups and click **Check Status.** An example of the output is shown in the image below. You now have a Snort sensor monitoring your network that is connected to enp0s3. Take a screen capture of your output and paste it in the Module 2 PowerPoint template.



**Part 2: Testing Snort Rules**

We have Snort set up now, but we need to do some testing. To the right of the sensor is a menu to set the Snort IDS action.

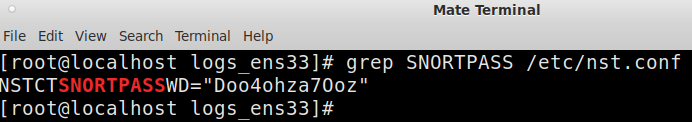
1. Click on **Rules**. An example of the Rules menu is shown in the image below. Check the **scan** option. Note that the scan setting is not enabled by default, and we enabled it here for our testing.



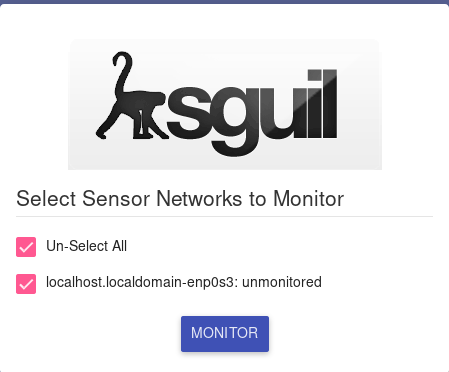
1. Take a few minutes and review the rules list. Click on a rule to review how the rules are written. Later we will be creating a custom rule.

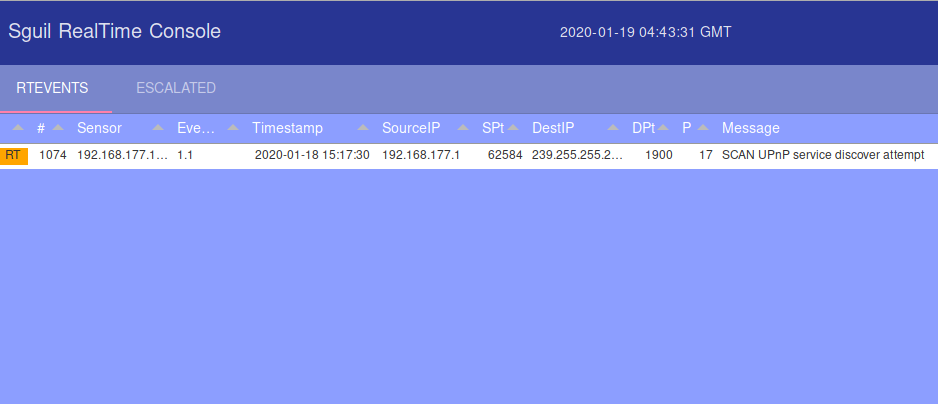
With this version of the Network Security Toolkit we will use Sguil (pronounced sqeel) for our database and GUI display. Before we access it, we need to determine what the password is because it is assigned randomly.

1. In the terminal window enter **grep SNORTPASS /etc/nst.conf**. The output is shown in the image below.

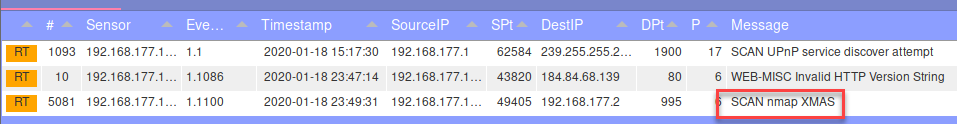


1. Click on the **Security | Intrusion Detection – Sguil | Sguil Web.** Enter the username **sguil** and the password that you discovered with the grep command above.
2. Once log in you should see the dashboard as shown below. Select the sensor network to monitor.





1. If you see the UPnP alert, that is a false positive and you can ignore it. Obviously, we would need to tune the sensor.
2. With the sensor working, we want to generate an attack. Switch to the Ubuntu-Web machine and open a terminal window. Enter **sudo** **nmap -n -sX 192.168.177.0/24**. This will perform an XMAS scan with Nmap and should generate alerts.
3. After the scan has ran for a few minutes, return to the Sguil dashboard and see what alerts are generated. An example of the display is shown in the image below.



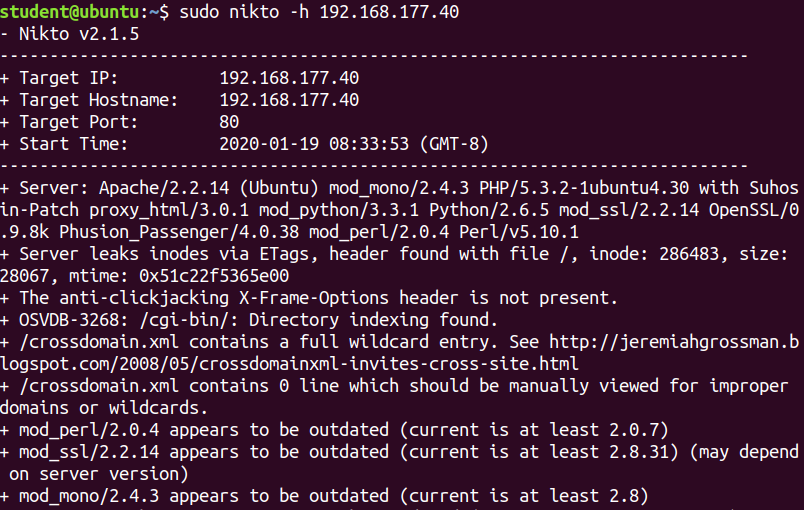
We have detected the XMAS scan with the sensor we just created!

1. If you select an Alert you can see the signature that generated the alert as if there is a payload. An example of this is shown in image below.

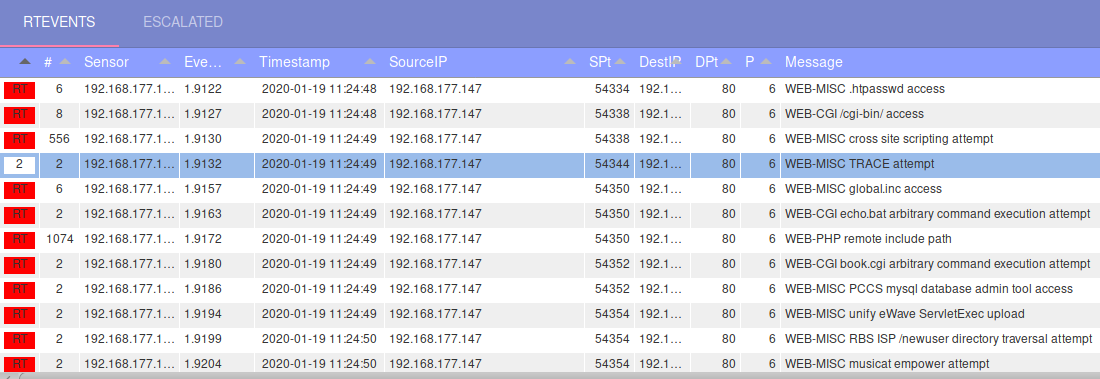


We want to generate some more attacks and test our sensor by using Nikto. The Nikto tool is based on the first web scanner that was ever built. This scanner was called Whisker and written by a hacker who goes by the name Rain Forest Puppy or better known as RFP. He got tired of maintaining the program, but others took what he had and improved on it to create Nikto. You can read more about it on the <https://cirt.net/> site.

1. Power on your **OWASP BWA** (also known as **DMZ-Machine**) machine. We need a web server as a target to test the sensor.
2. There is no need to log into the machine unless you need to discover the IP address. In our example, the IP address is 192.168.177.40. If yours is different, replace the IP address with your machine’s IP address.
3. On your Ubuntu-Web machine, enter **nikto -h 192.168.177.40 (**or IP address of your OWASP machine).A screen capture of the scan in progress is shown in the image below.



1. Once the scan finishes, return to the NST30 machine and check the Sguil dashboard. An example of the display is shown in the image below. Take a screen capture of your output and paste it in the Module 2 PowerPoint template.



Now we have lots of alerts because Nikto is actually running attack strings. The Nmap scan earlier was just reconnaissance. We do not want to have alerts for recon all the time, so there were only a few alerts.

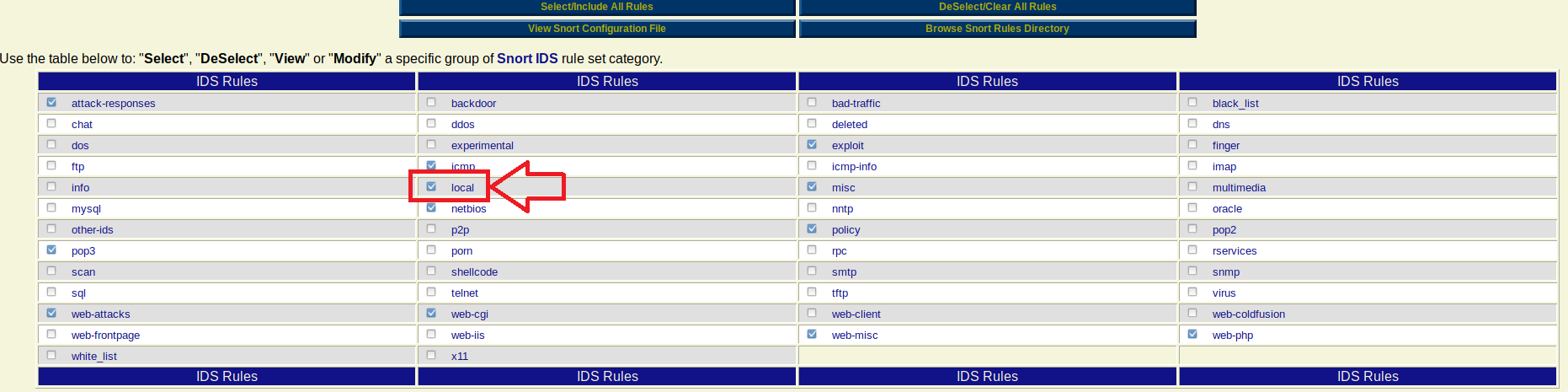
**Part 3: Creating Custom Snort Rules**

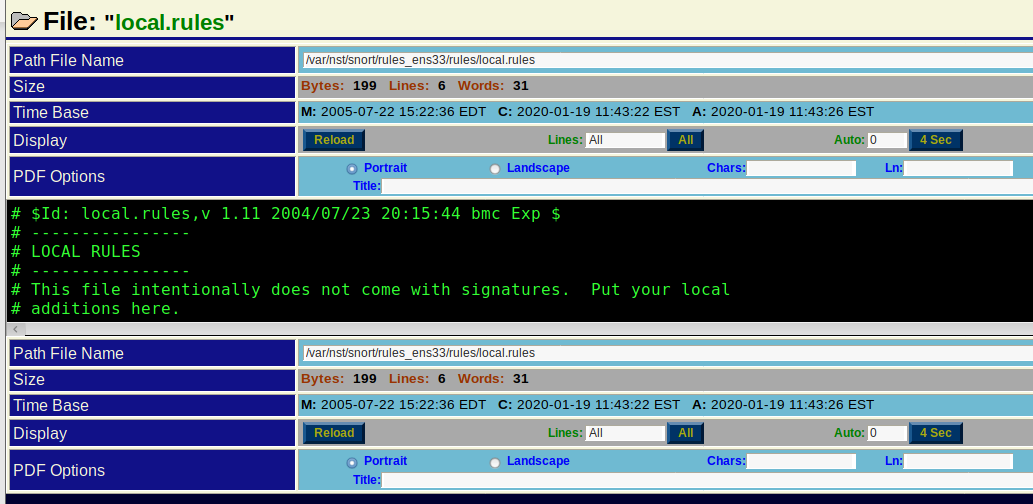
Let’s create our own custom rule and test it for Snort. The rules that are created in Snort are placed in the local.rules file and reloaded onto the Snort sensor.

1. Return to the Manage Snort IDS screen by clicking **Security | Intrusion Detection | Snort IDS – Sguil**. An image of where you want to be is shown below.

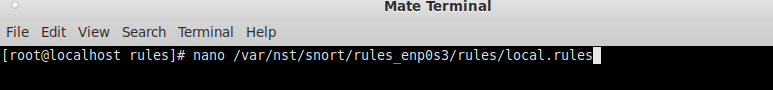


1. Click on **Rules** to open the rules listing. Then click on the **local** rule name. An example of the result is shown in the image below. This is where we put our additional rules.





1. Open the local rules file in nano, as shown in the image below.



1. Once the file is open, enter the following for your rule.

**alert ip any any -> 172.16.0.50 445 (msg: "CRITICAL ALERT";SID: 1000002; rev:1;)**

This alert is for any IP protocol destined to our OWASP BWA machine on port 445. We will see the weaknesses and attacks against this port and service later. Note that it is the Windows NetBIOS port for local communication. Because the OWASP BWA machine is not Windows, any connection attempt to it will be considered an attack or at the very least reconnaissance.

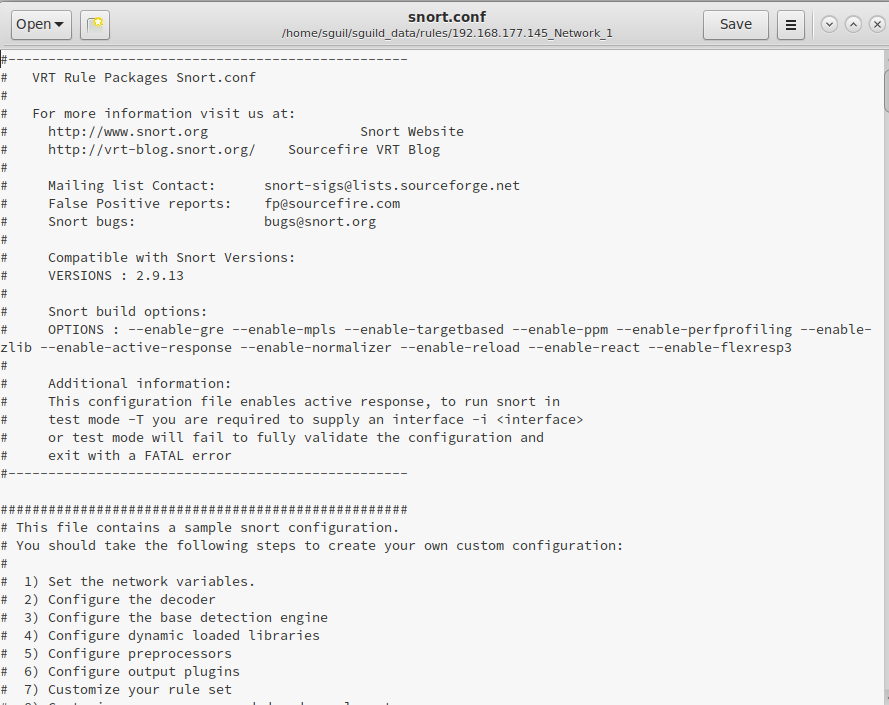
If your OWASP BWA Machine is on a different IP address, you will have to use it for your rule here. For details about the rule components, read the main page or do a search on the Internet.

1. Save the rule and reload your sensor before testing the newly created rule. Remember to select the radio button for the local rules and reload them (may need to type **setup\_snort -sig dump -i enp0s3 -v** on NTS Machine). If you get an error, go back and check your typing.
2. Once the sensor has reloaded from the Ubuntu-Web machine enter **sudo** **nmap -sS 172.16.0.50 -p 445.** An example of the output is shown in the image below. Take a screen capture of your output and paste it in the Module 2 PowerPoint template.



If you see the alert, you have just written a custom rule! One may ask why it is not stating what I placed in the text. This is because Sguil is using a database and your rule is not in the database. This is one of the downsides of GUI tools. The traditional Snort file is text based, and you would see whatever was in the rule text. Because this uses a database, we do not have that same capability. We know it is our rule by the ID of the alert.

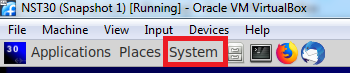
1. If you are curious, you can add the text-based output in the snort.conf file as shown in the image below. Once you open the file, just add the appropriate line. Down toward the bottom of the file are the output examples.



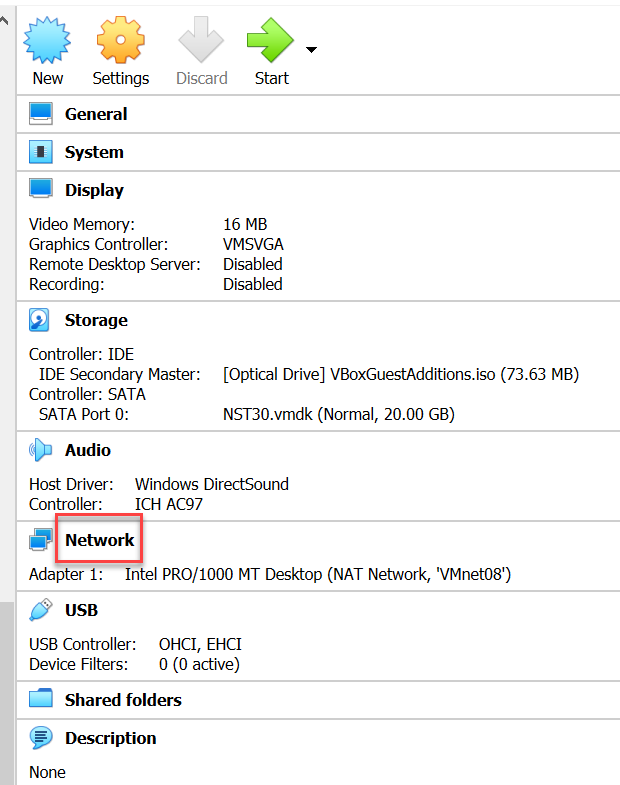
**Part 4: Deploying Multiple Snort Sensors**

We are now ready to configure additional sensors for the Snort deployment.

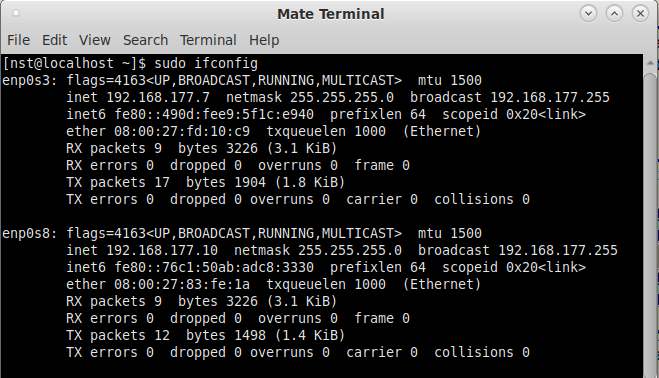
1. Click on **System | Shutdown** in your NST30 Machine.



1. Once the system has shutdown, click on **Network** in the machine configuration window as shown in the image below.



1. Once you are in the configuration, select **Adapter 2** from the top menu. Enable the network adapter and attach it to **Nat Network | VMnet08**.
2. Our demonstration has two sensors on the same network, which serves its purpose here. You could also change it to the network you wanted to monitor, and we will leave that as an exercise offline.
3. Power on the NST30 machine and log in with usrname/password **root/rootpw**.Open a terminal window and enter **ifconfig** to verify your settings have taken place. An example of the output is shown in the image below.



1. With the second network card being added, all we need to do is to bring it up in Snort. The steps were explained in Part 1. An example of what it looks like once you have both sensors up and running is shown in the image below. Take a screen capture of your output and paste it in the Module 2 PowerPoint template.



You could deploy sensors all around your network. A common way to use the Network Security Toolkit is with four network cards as sensors and one network card as out of band management.