[How to Evade a Network Intrusion Detection System (NIDS) Using Snort](https://null-byte.wonderhowto.com/how-to/hack-like-pro-evade-network-intrusion-detection-system-nids-using-snort-0148051/)

By [**occupytheweb**](https://creator.wonderhowto.com/occupythewebotw/) 08/13/2013 4:41 am

Nearly every commercial enterprise worth hacking has an intrusion detection system (IDS). These network intrusion detection systems are designed to detect any malicious activity on the network. That means you!

As the name implies, a network intrusion detection system (NIDS) is intended to alert the system administrator of network-based intrusions. As a hacker, the better we understand how these NIDS work, the better we can evade them and stealthily enter and exit a network without detection. In an attempt to train you to evade these systems, I am beginning new series on how NIDS work.

Introducing Snort: Our NIDS of Choice

**Snort** is an open-source NIDS that is the most widely used NIDS in the world. Some estimate its market share at over 60%. It's used by such large organizations as Verizon, AT&T, the U.S. State Department, most U.S. military bases, and millions of medium to large businesses around the globe. Last month (July 2013), Cisco announced that they would be acquiring the parent company of Snort, Sourcefire Inc. of Columbia, MD. This insures that Snort will remain the dominant NIDS on the planet for some time to come, making it increasingly important that we understand Snort—so we can evade it.



*Image via* [*wordpress.com*](http://wordpress.com)

Fortunately, Snort is built into our [BackTrack](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-backtrack-your-new-hacking-system-0146889/), so we don't need to install it. If you do need to download it, you can find it [here](http://www.snort.org/).

Step 1 Fire up Snort

Snort is basically a network traffic sniffer that can apply rules to the traffic it sees to determine whether it contains malicious traffic. We can start Snort in sniffer mode by opening any terminal in BackTrack and typing:

* **snort -vde**



After we hit enter, we begin to see packets going past the screen in rapid succession. Snort is simply sniffing packets from the wire and displaying them to us.



To stop Snort, hit the **Control C**. When we stop Snort, it displays our statistics on the packet capture.

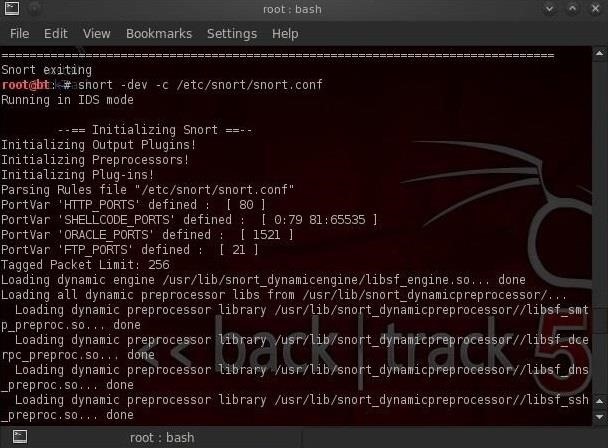
Step 2 Intrusion Detection Mode

To get Snort to operate in Intrusion Detection (IDS) mode, we need to get Snort to use its configuration file. Nearly all applications in [Linux](https://null-byte.wonderhowto.com/how-to/linux-basics/) are controlled by a configuration file that is a simple text file. This same applies to Snort. Snort's configuration file is named **snort.conf** and is usually found at **/etc/snort/snort.conf**. So, to get Snort to use its configuration file, we need to start it with:

* **snort -vde -c /etc/snort/snort.conf**

Where **-c** says use the configuration file, and **/etc/snort/snort.conf** is the location of the configuration file.

When Snort starts in IDS mode, we begin to see a screen similar to that below. Eventually, the screen will stop scrolling and Snort will begin to watch your network traffic.



Now Snort is sniffing our wire and will alert when something malicious appears!

Step 3 Configuring Snort

Snort comes with a default configuration file that, for the most part, will work with little editing. The configuration has plenty of comments to explain what each line and section does, so you can figure it out with little outside assistance.

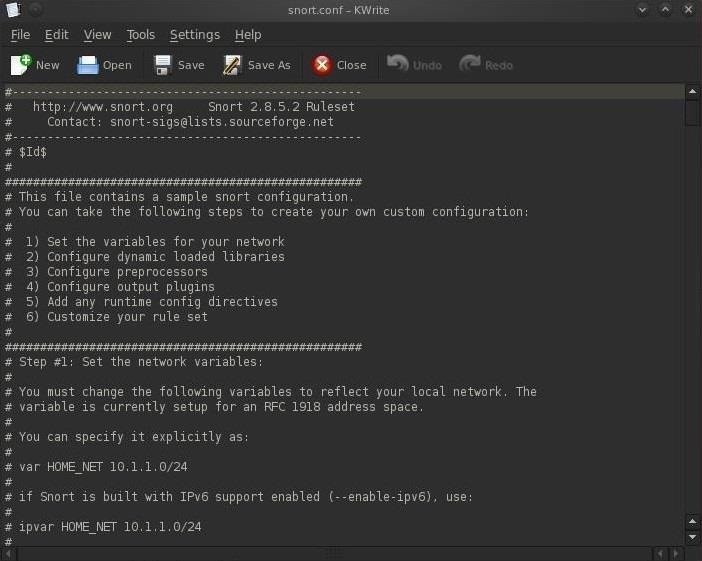
There are at least 3 areas, though, that need some attention and configuring...

1. The EXTERNAL\_NET variable
2. The HOME\_NET variable
3. The path to the Snort rules

Without the Snort rules, Snort is just a sniffer/packet logger, far from the powerful IDS it can be. That being said, let's get inside that Snort configuration file and make the minimum changes to get Snort to run as an effective IDS.

Let's open the snort configuration file with [**KWrite**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-backtrack-your-new-hacking-system-0146889/).

* **kwrite /etc/snort/snort.conf**



As you can see in the screenshot above, the configuration file is comprised of six (6) sections.

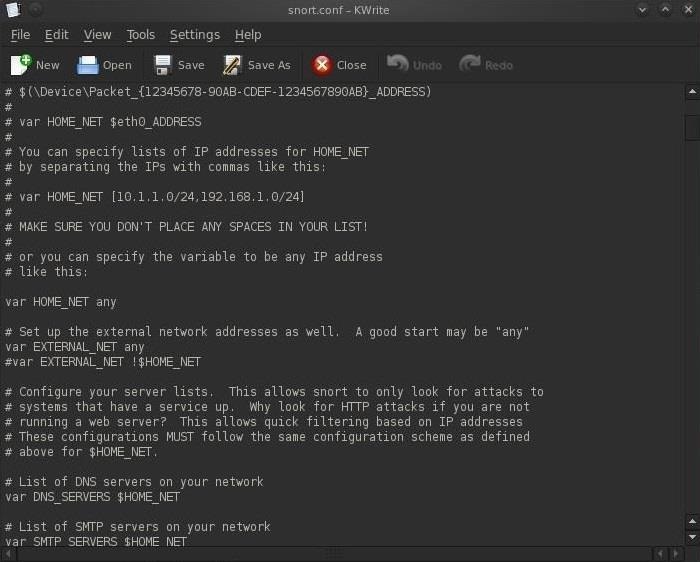
1. Set the variables on your network
2. Configure dynamic loaded libraries
3. Configure preprocessors
4. Configure output plugins
5. Add any runtime config directives
6. Customize your rule set

We need to first set the variables for our internal and external network. These are defined by the lines:

* **var HOME\_NET**
* **var EXTERNAL\_NET**

We can define our **HOME\_NET** as the IP address or subnet we're trying to protect. You see in the screenshot that it's set as "any." This will work, but it's not optimal for detecting malicious activity. We should set the **HOME\_NET** to our internal IP address, such as 192.168.1.1, or our internal subnet, such as 192.168.1.0/24.

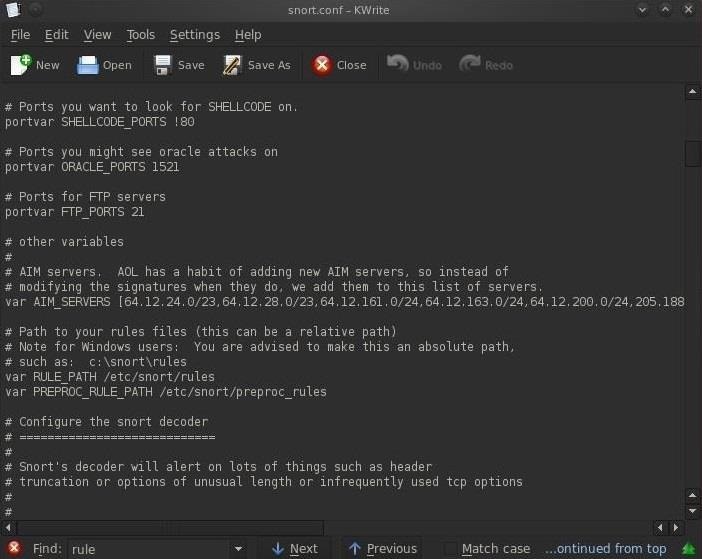
In most cases, security admins will define their **EXTERNAL\_NET** as everything that is NOT their **HOME\_NET**. To accomplish this, we can simply negate (**!**) the **HOME\_NET** or **! HOME\_NET**.



Next, we need to set our path to our rules. As we can see in the screenshot below, about two-thirds of the way down, there is:

* **var RULE\_PATH /etc/snort/rules**

In most installations, this path will be correct (but does vary with different installations) and we can simply leave it as is, but make certain that your rules are in this path before assuming so. When you are done, simply save the snort.conf file.



Step 4 Checking the Snort Rules

We can navigate to the rules directory by typing these two commands:

* **cd /etc/snort/rules**
* **ls -l**

In this way, we can see all of the files that comprise our Snort rules. It's these Snort rules that are designed to catch intrusions and alert the security admin.

