Guide To Using Snort For Basic Purposes

Author: delete852

Published: Sunday, 20 April 2003, 05:49 GMT

By Revenge (delete852-at-yahoo.com)

A few months ago I was presented with a task of creating a secure DMZ with Linux servers in it, since I am not a Linux guru yet, I wanted to research different programs and told that I can use to monitor, filter, traffic, as well as some other programs, but it doesn't matter right now. By my friend's recommendation I decided to look into snort as an IDS (Intrusion Detection System). In the following essay I will tell you about writing rules and alerts for snort. I went through a lot of reading and nights of trying to configure it, and playing around with it, and I think that if material was presented in a slightly different fashion if could of made the life of snort users much easier, and so here is some basic information first.

Well an Intrusion Detection System is used to monitor the traffic on your LAN, it wouldn't do anything to filter it, but it will log what you tell it to. So in case of a break in you will be able to go back through the packets that entered and see who performed what attack on your network. There is also DIDS, which is Distributed Intrusion Detection System, which spans over multiple sites, so if an intruder was breaking into your office in New-York, and then in a different office in Miami, you would be able to see him, in one central location, basically if you have 3 sites, you can set up all 3 of them in a special mode, where 2 of them would send their logs to the first one so you can look at all of them together. I will post a link on this later where you can find more information about this subject.

I am not going to go through the installation, since there is a guide already on www.snort.org, and since I am a debian user ;-) all I have to do is apt-get install snort* to have it installed (HINT: Debian roxors).

So at this point I assume that you have a working Linux computer with snort installed. So go ahead and do a "man snort" and read the manual. I really hate when people point to other guides in theirs, but there is no point in me telling you every flag, as I go along I will probably mention some of them anyway, but that's where you go for more information on different flags.

When you execute snort with -v flag it means in verbose mode and it will type all the headers of packets out to your screen, and with -d option it means to actually display the data that transmits, but it gets even better, if you execute:

snort -dev
you can see the whole thing, the header, and the content, and a bunch of other stuff. Cool huh? I spent about an hour once looking at different packets that were coming into my system, from different servers, mirc, aim, I was pretty bored.

So now lets try to get it to log stuff, depending on the way you installed this, it might be different but in debian it went the default way so that's the way I am going to explain it. There is certain flags that you use in order to make it log. There is this one flag "-A" and it is used to put it in alert mode, there are some options for it

-A fast
timestamp, alert message, source and destination IPs/ports
-A full

everything, and its the default one, I recommend using this one
-A none
turn off alerting

So try to to run snort -A it if gives you some error and its something about a config file missing, then do the following:

snort -A full -c /etc/snort/snort.conf

The -c flag tells snort where to find the config file, in the default installation that's where it goes. Now the best way to execute this command is with a & thing at the end which tells the shell to execute it in the back ground so you don't have to start another window and su to root.

So now that we have snort running and logging packets it is time to check some stuff it logged out, but first while its logging go and read /etc/snort/snort.conf, and read some rules, and see if you can get familiar with anything, its not that hard, but I don't want to reinvent the wheel and retype all that stuff. It is basically different variables, and some include files, since they don't want all these alerts in snort config file because it would be hard to modify and keep up with, they made include command which includes other files just like when you put include in the beginning of a C program to include a library module you do this the same way. There is a sample config file at

But anyway the alerts are just like packets from the -dev flags on snort, but they give you a little more detail for example they give you the name of alert so you know what type of attack it was, and what kind of packets the attacker was sending to your server. If you didn't get any alerts yet then be thankful, but if you leave it running for a few hours I am sure you ll fish out a whole bunch of them

so you guys can check it out if you whish. So if you check out the directory where the snort config files resides, which is /etc/snort you can see other directories with the files in them. Sometimes if you have a windows workstation and the linux server is on the same network as you are you can do the following:

```
/snort_conf snort.conf -b IM_WORKSTATIONS
```

Well now that it has been logging for a few minutes lets hop in /var/log/snort and see what we can come up with. First of all I would like to point your attention to the alerts file, that file is going to be your next best friend, because when an alert happens and there is a strange packet in your network that's where the alert will go, a good habit is to keep the size of it in mind, so next time you look at it, you can see if it was modified, and if the size went down that will send the send the alert message to windows workstations view WinPopUp, but you need samba configured in order for this option to work, and you have to have -enable-smbalerts switch when configuring snort. something might have happened, and you should investigate a little more.

But anyway back to alert, it is more or less self explanatory but I ll talk about it a little any way, first of all there is the alert message, (which in the actual alert script is msg: name of alert;) then there is some other stuff.....here is the one I got at some point in my alert file:

```
[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/30-19:35:54.306411 68.153.97.216:4464 -> 192.168.1.1:80
TCP TTL:122 TOS:0x0 ID:2271 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x949963A3 Ack: 0xA3F9CDE1 Win: 0x4510 TcpLen: 20

[**] [1:1002:2] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
03/30-19:35:54.555283 68.153.97.216:4477 -> 192.168.1.1:80
TCP TTL:122 TOS:0x0 ID:2302 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x94A46F43 Ack: 0xA3CF89A0 Win: 0x4510 TcpLen: 20
```

As you can see the attacker was trying to run a Code Red exploit on my machine, oh by the way there is an option for snort to take out your home network from the IP's in case you want to paste them somewhere like I did right now, but I don't give a shit since its my private LAN, and I am behind a router firewall, and plus I would log everything that you send to my network with snort ;-).

So these are examples of alert entries in your alert file. It is really very easy to look at them, its self-explanatory. Sometimes at the end there might be a URL that will tell you where you can find more information about it.

All right one of the most advanced parts of snort is being able to write rules and alerts. Since snort is used to monitor packets you can set up specials triggers, which once activated will perform a certain function, like write to a file, or to a terminal, etc. All the alerts that you write will go to a file in snort directory which is usually /etc/snort/snort.conf along with all other configuration parameters that you like. Here is a sample rule for snort:

alert tcp any any -> $HOME_NET any (content:"|00 01 86 a5|"; msg: "mountd access" ;)

In the latest release of snort you are able to extend the rule to 2 lines by putting a at the end of the line, and continuing at the next one. And you can also set variables, in my example $HOME_NET is a variable, so in snort.conf you should have:

var HOME_NET (192.168.1.0/24)

Its a good idea to have your home networks in a variable, as well as your external networks, but there is a shortcut for that, which I ll show you a little later. You can also launch snort in different options by putting stuff in config file, but you don't really need that since you are going to be using the flags. But just in case you want to, there is a list of them in snort's user manual. The reason I don't like to put things in config file is because sometimes you might want to launch snort in a different mode, with just a single command when time is of a factor. And editing the file will be a pain in the ass, so that's my reason.

Anyway, snort rules are divided in two sections the rule header, and rule option, rule header just basically specifies what kind of traffic this applies to, and packets with what addresses to scan. So:

alert tcp any any -> 192.168.1.0/24 111

is the rule header telling to scan packets coming in from anywhere with the destination for 192.168.1.0/24 on port 111. The arrow points the direction of the traffic, you can also have which means that it doesn't matter which way the traffic goes. Any represents any IP address, and the second any represents ay port number. The very first word is the type of alert and the second one is the protocol that you want to look at, so in this case it is tcp.

(content:"|00 01 86 a5|"; msg: "mountd access";)

This is the rule option, this tells exactly what to do with the packet once it fits the rule header which is all the IP stuff. The content word makes snort look for the following hex characters in the packet that statement is ended by a ; and it symbolizes that a new statement is going to begin after the ; and it does, the next statement is msg which means to write the following alert into the file. The words before the colon (ie. content and msg) are called option keywords, they always appear, sometimes more than once, and always have a colon after them, then space and the value in double quotes.

There is the alert keyword that you noticed which was just the very first word in the line, that is called the rule action, this specifies what exactly to do, there are 5 things that can be done I will mainly cover 3, and touch up on other 2, here they are:

alert - send alert to the file, and then log the packet
log - just log the packet
pass - which is ignore the packet; drop
activate - just like alert
dynamic - when a series of things trigger this it activate an active rule header

So after you chose your alert keyword you need to choose the protocol, the following protocols are supported, TCP, UDP, and ICMP. In the future some routing protocols can be added to it as well. The next comes the IP addresses to match, you can use any to get any address, or you can use something like this:

alert tcp !$HOME_NET any -> $HOME_NET any ...

The ! Means that it should be everything except that, so that line will listen for any packets coming into your network from outside. It is better than any because any would also catch you sending them the packets and sometimes you don't need that, and you only need the once with the source address different from the one in your network.

Once you put in the source IP you need to specify which ports to listen on, you can also do an any command and it will listen for any ports, you can set a range like so.

"1:10" will listen on any ports from 1 to 10
or like this
":1024"
that will listen on all ports smaller than 1024. Get the drift?

So to have some hands on lets try doing the following and seeing what happens, go ahead and open up your snort configuration file with your favorite editor, I like nano because it is easy to use, and I kind of already have it so I would do the following command:

nano /etc/snort/snort.conf

and than opens up snort config file. The next step is write the alert to it, lets write the following lines in it:

Look for any packets coming in to your network
alert tcp any any -> $HOME_NET any
(content: "Yahoo"; msg: "Yahoo Website Access";)

Now save it, and do the following command:
snort -A full -c /etc/snort/snort.conf

That command launches snort in full alert mode pointing to the config file that we just edited.

Now lets see what happens when you go to yahoo.com So go ahead and open up your web browser and go to yahoo.com. Nothing right, it opens up as usual and nothing different happened. Ok, so now go ahead and look at your alert file, you will see something like:

```
[**] [1:0:0] Yahoo Website Access [**]
04/14-19:44:54.571931 216.109.125.72:80 -> 192.168.1.1:32802
TCP TTL:46 TOS:0x0 ID:51401 IpLen:20 DgmLen:1492 DF
***A**** Seq: 0x668B0B47 Ack: 0x833208B7 Win: 0x8160 TcpLen: 32
TCP Options (3) => NOP NOP TS: 232478239 85744
```

Ok now hold up....What just happened? Let me explain, well the string that we put in the config file said that snort should inspect any packet coming in from any ip address, and from any port. And then if it finds "Yahoo" in the packet it should log it. And then following that we gave the following command

msg: "Yahoo Website Access";
that just told snort that when it finds "yahoo" in a packet it should send in alert and called it Yahoo Website Access.

Just with these two functions you can see how powerful snort really is.

Here is a list of all 15 of snort's rule options. This list is taken from http://packetstormsecurity.nl/papers/IDS/snort_rules.htm it is a snort tutorial by Martin Roesch, I found it very helpful in learning different functions of snort and I also recommend reading it once you are done with this one off course ;-).

msg - prints a message in alerts and packet logs
logto - log the packet to a user specified filename instead of the standard output file
minfrag - set a threshold value for the smallest acceptable IP fragment size
ttl - test the IP header's TTL field value
id - test the IP header's fragment ID field for a specific value
dsize - test the packet's payload size against a value
content - search for a pattern in the packet's payload
offset - modifier for the content option, sets the offset to begin attempting a pattern match
depth - modifier for the content option, sets the maximum search depth for a pattern match attempt
flags - test the TCP flags for certain values
seq - test the TCP sequence number field for a specific value
ack - test the TCP acknowledgement field for a specific value
itype - test the ICMP type field against a specific value
icode - test the ICMP code field against a specific value
session - dumps the application layer information for a given session

These rule options are pretty much self explanatory so I will not go in detail about each one.

Some good things to keep in mind is that rules are case sensitive, so Yahoo and yahoo isn't the same thing. And it wouldn't get logged! The good thing that I didn't think right away is that snort already comes with a shipload of built in rules. So you don't have to write every single one, it already detects most things, all you have to do is just to pay attention to them, and write new once as new exposits come out. There are also other tools that would convert logs into HTML file formats for better management, but that's a topic for another tutorial. TIll then, enjoy, and have happy logging.

Shot Outs to: Blaza7021, Fire332211, ambush, Jennifer, SK!l!NE, Shaolin Tiger, saxo, fastlawn, the kingster, wombat, bigbadapeone, cire668, Liquid Fish, myhatisred, Z-lite, PCWriter, Wings, and the rest of the folks on www.security-forums.com, and in Urban Vendettas, as well as the dead r00t-access crew. If you go to my school and your name isn't on there, it means I don't like you. Yes that means YOU!

image:rdf newsfeed / //static.linuxhowtos.org/data/rdf.png (null)
|
image:rss newsfeed / //static.linuxhowtos.org/data/rss.png (null)
|
image:Atom newsfeed / //static.linuxhowtos.org/data/atom.png (null)
- Powered by
image:LeopardCMS / //static.linuxhowtos.org/data/leopardcms.png (null)
- Running on
image:Gentoo / //static.linuxhowtos.org/data/gentoo.png (null)
-
Copyright 2004-2020 Sascha Nitsch Unternehmensberatung GmbH
image:Valid XHTML1.1 / //static.linuxhowtos.org/data/xhtml.png (null)
:
image:Valid CSS / //static.linuxhowtos.org/data/css.png (null)
:
image:buttonmaker / //static.linuxhowtos.org/data/buttonmaker.png (null)
- Level Triple-A Conformance to Web Content Accessibility Guidelines 1.0 -
- Copyright and legal notices -
Time to create this page: ms
<!--
image:system status display / /status/output.jpg (null)
-->
bodyloaded();