By Ryan
Published: 2007-12-21 16:33

Writing Snort Rules On EnGarde Intro:

There are already tons of written Snort rules, but there just might be a time where you need to write one yourself. You can think of writing Snort rules as writing a program. They can include variables, keywords and functions. Why do we need to write rules? The reason is, without rules Snort will never detect someone trying to hack your machine. This HOWTO will give you confidence to write your own rules.

Prerequisites:

What you will need:
- A machine to do your development on. These rules should NOT be run on a production server because the rules are only meant to be examples, which you can learn from.
- Also you will need a client machine to connect to the machine which Snort is running on.
- EnGarde Secure Community 3.0.18 or above with Snort installed.

Syntax: The Guts of Rules

The syntax may look a little strange at first but this section will explain it so you can start writing your own rules. Snort rules are divided into two sections: the ***rule header*** and the ***rule options*** . First, the ***rule header*** contains rules, actions, protocol, source and destination IP address, and source and destination ports. The second part is ***rule options,*** which contains an alert message and information on the parts of the packet that should be looked at to see if the rule action should be taken.

Example:

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)
```

The text up to the first parenthesis is the ***rule header*** and the section inside the parenthesis is the (***rule option*** s). ***Rule Actions:***

This is where you describe the œwho, where, and what• of a packet and what to do in the event that the rule is triggered. You can choose from the below

keywords when writing the ***rule action.***

alert: generate an alert using the selected alert method, and then log the packet

log: log the packet

pass: ignore the packet ***Protocol:***

Next part of the rule is the protocol. The more popular ones are: TCP, UDP and ICMP but Snort supports many other and continues to add new ones.

Source IP Address:

Following the protocol is the source IP address. This defines where the packet is coming from. You can use the keyword ***any*** to define all IP addresses. You can even write a rule to match any address except the one that you defined. This is done by using œ!•, the negation operator ***Source Port :***

This is the port number where the packet is coming from. Port numbers also have the keyword ***any*** . You can also define a range of ports. This is done by using œ:•. For example 1:1000 defines all ports ranging from 1 to 1000. ***Direction Operator:***

The direction operator œ->• is used to define the œdirection• of the traffic in which the rule applies to. In other words, where the traffic is coming in or out of your machine. ***Destination IP Address:***

Next is the destination IP address. Which defines where the packet is going too. Similar to the source IP address you can use the keyword ***any*** or define a address which will not cause the rule to be triggered. ***Destination Port :***

Following the destination IP address is the destination port number. This is the port number where the packet is trying to connect to. The options here are the same as the source port. ***Basic format:***

```
action  protocol  src_ip   src_port  direction  dst_ip dst_port ( rule options)
```

Adding a New Rule:

Since we now have a basic understanding of the syntax of Snort rules, we can add a new rule to our system.

First log in as root and transition over to sysadm_r.

```
newrole -r sysadm_r
```

```
[test_server]# newrole -r sysadm_r
Authenticating root.
Password:
```

```
setenforce 0
```

Next you will need to edit the snort.conf, use your favorite editor to modify the */var/chroot/snort/etc/snort.conf*. We need to include the line below:
alert tcp any any -> any 80 (msg: "Sample alert";classtype:misc-attack; sid: 2002973; rev:1;)

Last restart Snort to have your new rule take affect. Rule we just added:***How the rules works:***

The above rule is triggered when a user tries to access a website. When the rule is triggered it will do an alert and display a message. The action keyword ***alert*** generates an alert using the defined method, and then logs the packet. The protocol of the packet we are detecting is TCP and all source IP addresses and port numbers are defined. The destination is defined on any IP address that is connecting to port 80. Lastly, the ***rules option*** keyword ***msg*** tells the logger and alerting engine to display the message œSample alert•. ***Testing:***

Now you must be interested in seeing your rule in action.

To see the rules firing you will need to tail the Snort alert logs.

```
cd /var/chroot/snort/var/log/snort
```

```
tail -f alert
```

Now open a web browser and enter your test_server's IP address.

Look at the Snort's alert logs. You will see a message from Snort that was cause by the new rule we just added.

```
[**] [1:2002973:1] Sample alert [**]

[Classification: Misc Attack] [Priority: 2]

12/12-15:35:22.130162 test_client:35524 -> test_server:80

TCP TTL:64 TOS:0x0 ID:35734 IpLen:20 DgmLen:52 DF

***A**** Seq: 0x5F3B46F0 Ack: 0x85067266 Win: 0xB7 TcpLen: 32

TCP Options (3) => NOP NOP TS: 49925498 1529581
```

Detecting Payload Example:

Add the below line to */var/chroot/snort/etc/local.rules*:

```
alert tcp any any -> any 80 (content:"index.pl";sid:12345678;rev:1;classtype:misc-attack;)
```

As you can see we wrote a rule to detect any traffic connecting to port 80 with the content of œindex.pl•.

To test this do the above steps to tail the Snort's alert logs. Then open a web browser and enter.

This is only the start:

With the knowledge you have now you can start digging deeper into the writing your own rules. The official Snort documentation contains every in and out of the syntax. As you journey deeper into writing your own Snort rules you will notice attackers on your network that you have never seen before.