% Security topics
%
% Basic Snort Exercise

Introduction

In this exercise we will set up Snort, a popular Intrusion Detection System, in order to demonstrate how to monitor traffic and receive alarms for network traffic patterns that could be related to an intrusion.

Notes

* Commands preceded with "$" imply that you should execute the command as a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

Goals

* Learn how to install the Snort package on Ubuntu
* Learn the locations of the different configuration files and logs
* Learn how to read alerts and identify rules that triggered them
* Learn how to disable rules and suppress alerts
* Use a port scanning tool to generate alerts on other PCs in the classroom

Installation

Log in to the PC assigned to you, and install the Snort package:

```
$ sudo apt-get install snort
```

You will see a window prompting you to provide the "Address range for the local network". Type the network address of your particular group.

For example, for the first group, the network block is:

    10.10.1.0/24

For the second group, the network block is

    10.10.2.0/24

etc...

Check that the snort deaemon is running:

```
$ ps -ef |grep snort
```

You should see something like this:

```
snort     1523     1  0 16:22 ?        00:00:01 /usr/sbin/snort -m 027 -D -d \
```

```
-l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf \
-S HOME_NET=[10.10.1.0/24] -i eth0
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

The configuration is read from the file /etc/snort/snort.conf, which we discuss below.

Notice the variable "HOME_NET". It should reflect the value you used for your network during the installation.

Also, notice that the logs are sent to "/var/log/snort".

The Ubuntu package creates an additional configuration file that you should know of:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cat /etc/snort/snort.debian.conf
# This file is used for options that are changed by Debian to leave
# the original lib files untouched.
# You have to use "dpkg-reconfigure snort" to change them.

DEBIAN_SNORT_STARTUP="boot"
DEBIAN_SNORT_HOME_NET="10.10.1.0/24"
DEBIAN_SNORT_OPTIONS=""
DEBIAN_SNORT_INTERFACE="eth0"
DEBIAN_SNORT_SEND_STATS="true"
DEBIAN_SNORT_STATS_RCPT="root"
DEBIAN_SNORT_STATS_THRESHOLD="1"
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Operation

Overview

Let's take a look at the logs directory:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ ls -l /var/log/snort
total 8
-rw-r--r-- 1 root  adm 371 2012-03-12 16:39 alert
-rw-r----- 1 snort adm 106 2012-03-12 16:39 tcpdump.log.1331569367
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

The file "alert" is where Snort will write its alert messages when the traffic on eth0 matches patterns in one of the configured rules.

The other file "tcpdump.log.*" is a binary file in tcpdump capture format. Let's see what is in that file. We need to install tcpdump first.

NOTE: YOU MAY NOT HAVE ANY ALERTS YET. This is just an example. Keep reading!

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install tcpdump
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Now, if you do have a file under /var/log/snort/, let's use tcpdump that we want to read the packets stored in that file.

Now, let's use tcpdump:

~~~~~~
$ sudo tcpdump -nv -r /var/log/snort/tcpdump.log.1331569367
~~~~~~

Result:

~~~~~~
reading from file /var/log/snort/tcpdump.log.1331569367, link-type EN10MB \
(Ethernet)
16:39:33.296390 IP (tos 0x0, ttl 64, id 39949, offset 0, flags [DF], proto \
TCP (6), length 52)
    10.10.1.1.33154 > 10.10.0.250.3142: Flags [.], cksum 0x1b59 (correct), \
ack 1505459219, win 5208, options [nop,nop,TS val 1533593 ecr 20155833], length 0
~~~~~~

This is telling us that Snort found some traffic that matched one of its rules. In particular, TCP traffic from IP 10.10.1.1 going to 10.10.0.250, towards port 3142.

Let's see what is in the alert file:

~~~~~~
$ less /var/log/snort/alert
~~~~~~

You might see:

~~~~~~
[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy
[**]
[Classification: Attempted Denial of Service] [Priority: 2]
03/12-16:39:33.296390 10.10.1.1:33154 -> 10.10.0.250:3142
TCP TTL:64 TOS:0x0 ID:39949 IpLen:20 DgmLen:52 DF
A* Seq: 0xA6FCD5A Ack: 0x59BB7C13 Win: 0x1458 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1533593 20155833
~~~~~~

The first line is important. It's revealing information about the Snort rule that caused this alert. The numbers [1:100000160:2] represent [gid:sid:rev] where:

gid = Generator ID: Indicates what part of Snort generates the event
sid = Signature ID: Uniquely identifies Snort rules
rev = Revision: The version number of this rule

We can quickly determine the location of this particular rule by grepping for that sid number in the directory where Snort stores its rules:

~~~~~~
$ grep -r sid:100000160 /etc/snort/rules/*
~~~~~~

~~~~~~
/etc/snort/rules/community-sip.rules:alert ip any any -> any 5060 \
(msg:"COMMUNITY SIP TCP/IP message flooding directed to SIP proxy"; \
threshold: type both, track by_src, count 300, seconds 60; \
classtype:attempted-dos; sid:100000160; rev:2;)
~~~~~~

There's a problem with this rule. It says "alert ip any -> any 5060".
The problem is that it should be looking for TCP or UDP traffic destined to
port 5060, not just "ip" traffic.

NOTE: This rule exists in the Snort package for Ubuntu 12.04. It has been
removed in more recent versions of the package.

Supressing alerts

You will notice that Snort will initially generate lots of invalid alerts like
the one above (false positives). If your alerts file gets filled up with junk,
it won't be very useful, so you'll need to fine-tune Snort to suit your needs.

Method 1: Disable the rules file.

In the example shown above, all the rules in the file community-sip.rules are
incorrect. In that case, the easiest thing is to just not include that file
when loading Snort. For that, do the following:

~~~~~~
$ sudo editor /etc/snort/snort.conf
~~~~~~

find this line:

~~~~~~
include $RULE_PATH/community-sip.rules
~~~~~~

and comment it out like this:

~~~~~~
#include $RULE_PATH/community-sip.rules
~~~~~~

then, save and restart Snort

~~~~~~
$ sudo service snort restart
~~~~~~

Method 2: Supress the specific rule in the configuration file

* To suppress the above rule so that it doesn't match traffic from/to any hosts,
the configuration syntax is:

~~~~~~
supress gen_id <gid>, sig_id <sid>
~~~~~~

* If, on the other hand, you wanted to supress events from this rule that match
a specific origin or destination host, the syntax is:

~~~~~~
suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst>, ip <ip-list>
~~~~~~

Let's suppress events from our broken rule using the first option:

```
$ sudo EDITOR /etc/snort/threshold.conf
```

At the end of the file, add the following line:

```
suppress gen_id 1, sig_id 100000160
```

then, save and exit. Restart Snort

```
$ sudo service snort restart
```

Simulate intrusion attempts

Let's generate some traffic towards your classmates' networks in other groups.

First, install the nmap package:

```
$ sudo apt-get install nmap
```

Now we are going to scan all the TCP ports on another machine to see what could be potentially vulnerable.

NOTE: Change "X" to the number of a group in a network _other_ than your own. Otherwise, the alerts will not trigger because Snort is looking at traffic coming from EXTERNAL networks.

```
$ sudo nmap -sS 10.10.X.10
$ sudo nmap -sS 10.10.X.253
```

Repeat the above commands for as many hosts as you can (in other groups).

Wait a little bit, and check your alerts:

```
$ less /var/log/snort/alert
```

If someone is scanning your PC, you should start seeing some entries.

If not, ask a person from another group to scan your PC: remember that other people in the class may not yet be ready with the Snort part of their labs, so just ask them to scan you instead.

For example, you might find:

```
[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
```

```
03/12-18:30:21.185863 10.10.4.13 -> 10.10.1.1
ICMP TTL:55 TOS:0x0 ID:44605 IpLen:20 DgmLen:28
Type:8  Code:0  ID:3517   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS162]
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Let's see where that came from:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ grep 'sid:469' /etc/snort/rules/*
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

You should see something like this:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
/etc/snort/rules/icmp.rules:alert icmp $EXTERNAL_NET any -> $HOME_NET any \
(msg:"ICMP PING NMAP"; dsize:0; itype:8; reference:arachnids,162; \
classtype:attempted-recon; sid:469; rev:3;)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Here, the interesting information is "dsize:0". This alert is triggered when the size of the data in the ping packet is zero (0). The tool nmap typically pings the host via ICMP if the user has root privileges.

Also, you may see this in your alerts:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[**] [122:1:0] (portscan) TCP Portscan [**]
[Priority: 3]
03/12-18:30:21.305881 10.10.4.13 -> 10.10.1.1
PROTO:255 TTL:0 TOS:0x0 ID:0 IpLen:20 DgmLen:155 DF
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

If you try searching for this rule (122:1) in /etc/snort/rules, you will not find it. The reason is that this alert is not triggered by a standard rule but by a Snort "preprocessor". In these cases, you may find it easier to learn more about the mechanism that triggered this alert by searching the gid and sid in the snort search engine:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://www.snort.org/search/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

For example, you will find details about this alert by searching for "sid:122-1"

More information

The Snort website contains lots of useful information

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://www.snort.org
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```