Snort Lab

02.25.2020

CSC427

University of Toronto Mississauga

Overview

You will be using the Kali Linux virtual machine for this lab. The best way to learn how Snort works is to configure the rules yourself. You will take a look at the snort.conf file and learn to set up Snort. There are two parts to this lab which are laid out in Goals.

Goals

1. Part I Modify the snort.conf file and configure Snort.
2. Part II Create some Snort rules based on the requirements.
3. Submit the final work according to Submission.

Kali Linux

Create a new directory: `mkdir /virtual/UTORid/snort/`

Copy the VM to the directory you just created:

```
cp -r /virtual/csc427/snort/  /virtual/UTORid/snort/
```

User: root

Password: trysnort

Note: make sure to run VM in bridge mode.

Part I Configure Snort file

There are a few things to do before you can configure Snort rules. On your virtual machine, open up the Snort configuration file by using your favorite editor:

```
vi /etc/snort/snort.conf
```

Inside `snort.conf`, you need to do the following:

Step 1: Locate the `HOME_NET` variable, change the network address to the IP addresses you are protecting. It can be a single IP address or a block of IP addresses by specifying a CIDR block. For this lab, please setup the address to a block of IP addresses specific to your eth0. (Hint: reference the official Snort manual)

Step 2: Look for the variable `RULE_PATH`, this contains the path to some rules you have configured. Notice that the default path would not work, you have to inspect the file directory structure inside `/etc/snort/` to figure out the correct path.

Step 3: Uncomment the line `include $RULE_PATH/local.rules`, this is the file where your configured rules should reside.

Save and close the file.

Lastly, run `snort -T -i eth0 -c /etc/snort/snort.conf`. This is to validate the configuration file. If you are doing everything correctly, you should see the last two lines as:

```
Snort successfully validated the configuration!
```

```
Snort exiting
```

Part II Configure rules

To configure rules, you need to edit the file `local.rules`. Open up the rules file using your favorite editor. The path to this file should be clear after completing Part I.

Step 1: add a rule so that Snort will generate an alert with the message “new telnet connection attempt” if someone tries to Telnet to your machine’s address through port 80. (Hint: telnet runs on top of tcp)

Step 2: add a rule so that Snort will generate an alert if a packet arriving at port 80 has a payload that contains content “malicious”. (Hint: reference the Snort official manual).

Save and close the file.

Lastly, run Snort in IPS mode and tell it to output any alerts to the console by running the following command:

```
snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Now it will capture packets according to your rules and generate alerts to the console. Try to send those packets by yourself from another machine and see if your rules worked.

Submission

`snort.conf`: Submit a copy of your changed file.

`local.rules`: Submit a copy of your changed file.

Zip these two files as `snort.zip` and submit through UTORsubmit.