Objectives

In this lab students will explore the Snort Intrusion Detection Systems. The students will study Snort IDS, a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger. For the purpose of this lab the students will use snort as a packet sniffer and write their own IDS rules.

Software Requirement

All required files are packed and configured in the provided virtual machine image.

-The VMWare Software - http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The Ubuntu 14.04 or Ubuntu Long Term Support (LTS) versionor Kali linux image
- The Ubuntu 14.04 or Ubuntu 14.04 Long Term Support (LTS) Version
- Snort: A signature-based Intrusion Detection System https://www.snort.org/#get-started

Implementation

Starting the Lab 1 Virtual Machine

In this lab, we use Ubuntu as our VM image.

Login the Ubuntu image with username and password

Installing Snort into the Operating System

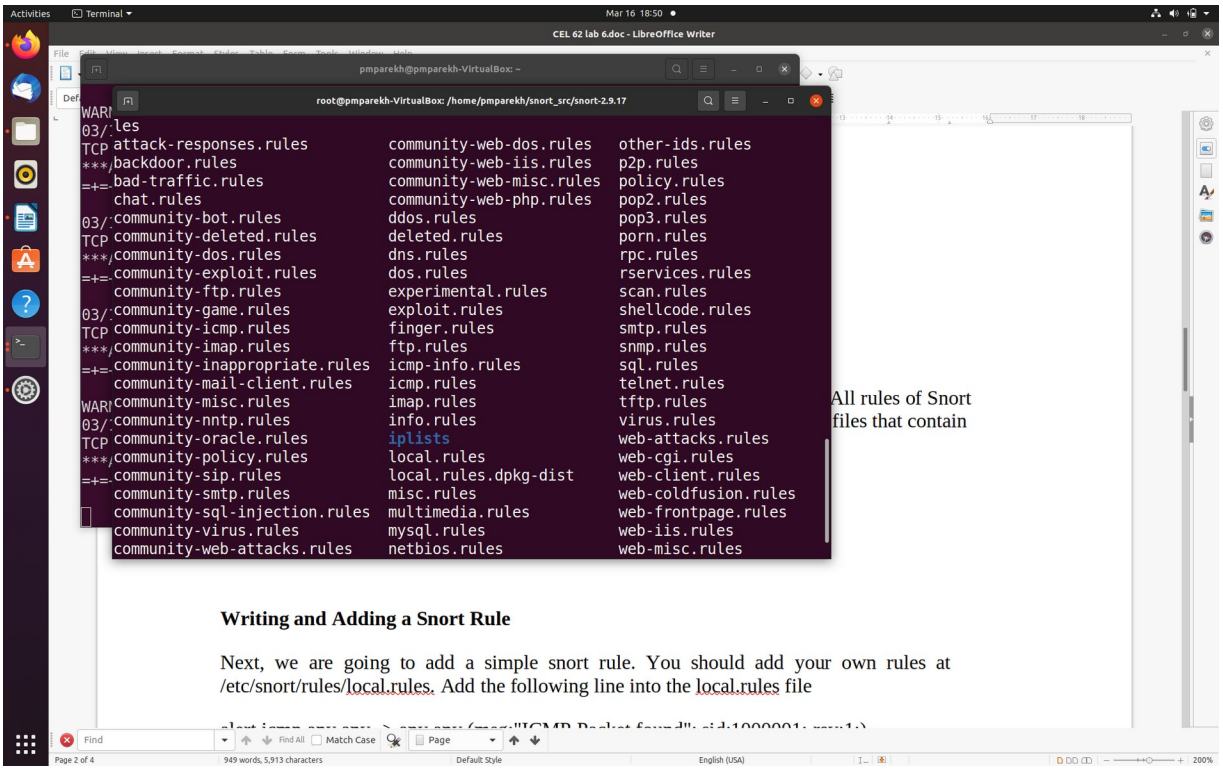
To install the latest version of the snort, you can follow the installation instruction from the snort website. Note that installation instructions are vary from OSes. The instruction below shows how to install snort from its source code on Linux.

You can find more information here:

https://www.snort.org/#get-started

While you install the snort, you system may miss some libraries. You need to install the required libraries, too.

Rules -



Snort is software created by Martin Roesch, which is widely used as Intrusion Prevention System [IPS] and Intrusion Detection System [IDS] in the network. It is separated into the five most important mechanisms for instance: Detection engine, Logging, and alerting system, a Packet decoder, Preprocessor, and Output modules.

The program is quite famous to carry out real-time traffic analysis, also used to detect query or attacks, packet logging on Internet Protocol networks, to detect malicious activity, denial of

service attacks and port scans by monitoring network traffic, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes:

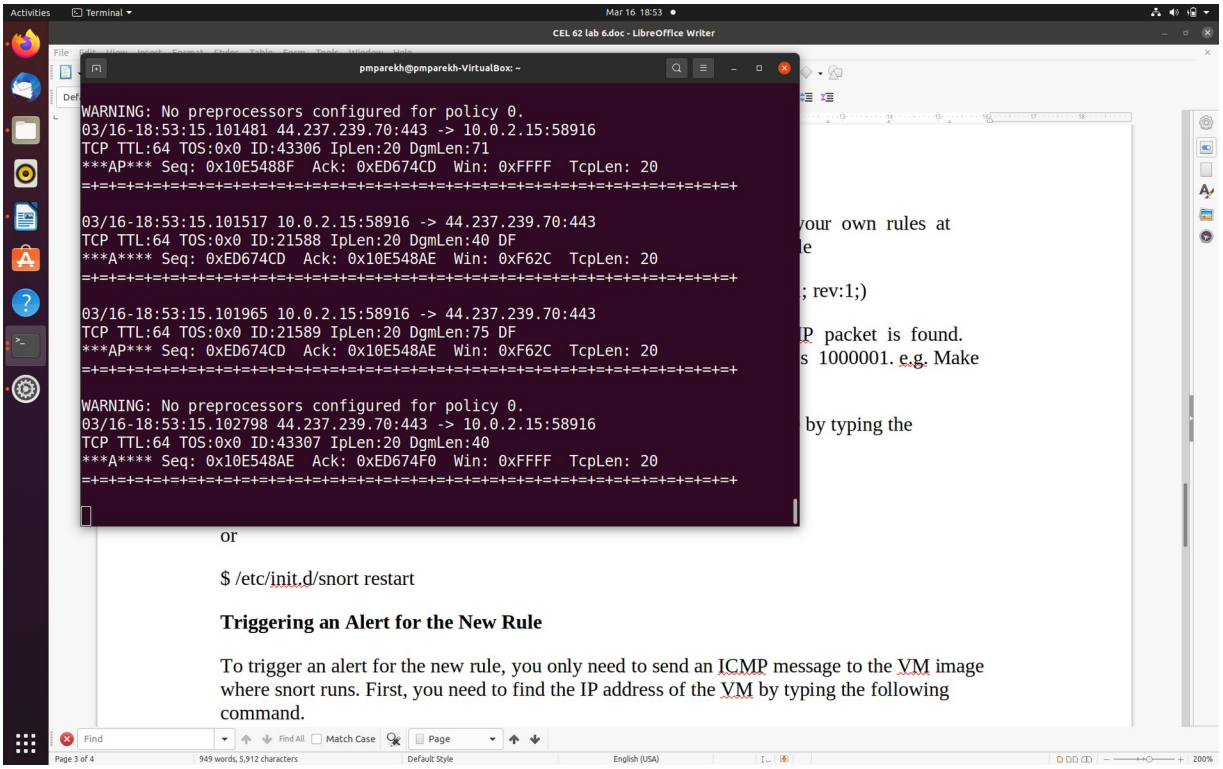
Sniffer mode: it will observe network packets and present them on the console.

Packet logger mode: it will record packets to the disk.

Intrusion detection mode: the program will monitor network traffic and analyze it against a rule set defined by the user.

After that, the application will execute a precise action depend upon what has been identified.

Starting of SNORT



Configuring and Starting the Snort IDS

After installing the Snort, we need to configure it. The configuration file of snort is stored at /etc/snort/snort.conf. The screenshot below shows the commands to configure the Snort. You need to switch to root to gain the permission to read the snort configurations file.

After configuring the Snort, you need to start the Snort. You can simply type the following command to start the service.

$ service snort start

or

$ /etc/init.d/

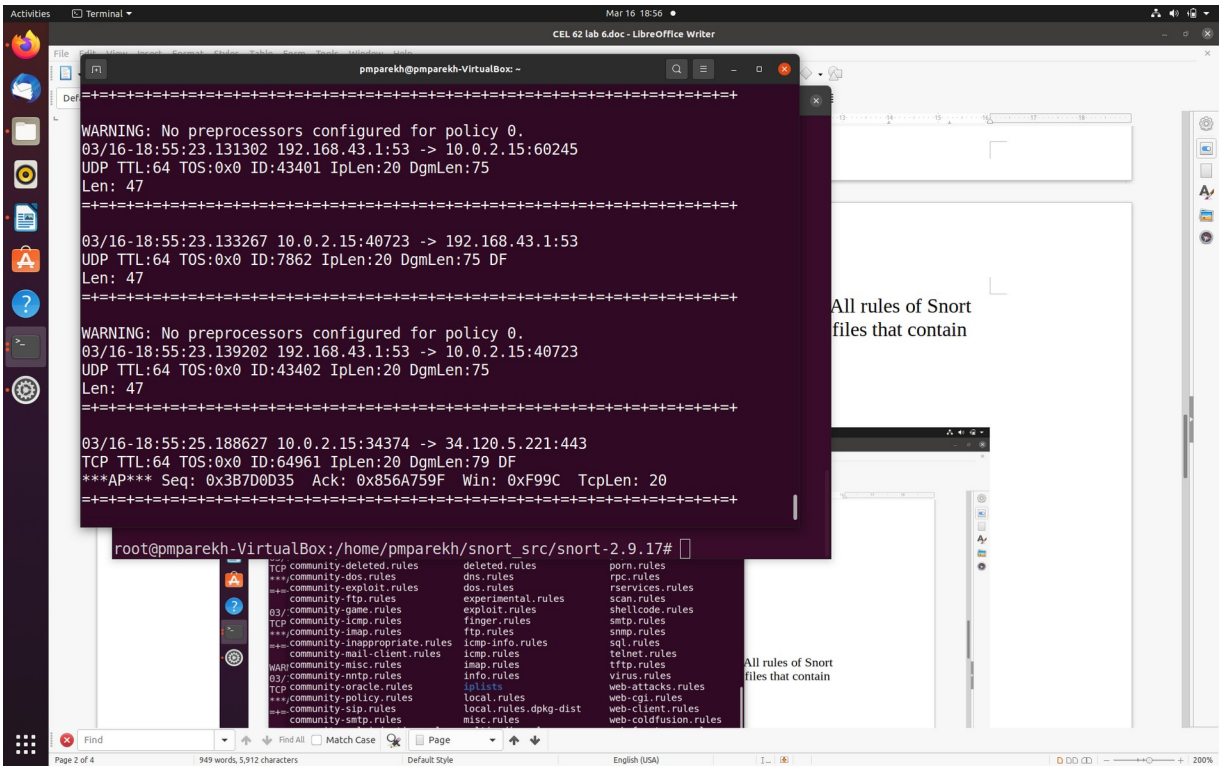
snort start

Snort Rules

Snort is a signature-based IDS, and it defines rules to detect the intrusions. All rules of Snort are stored under /etc/snort/rules directory. The screenshot below shows the files that contain rules of Snort.

$ ls /etc/snort/rules

Pinging with SNORT of Ubuntu from windows



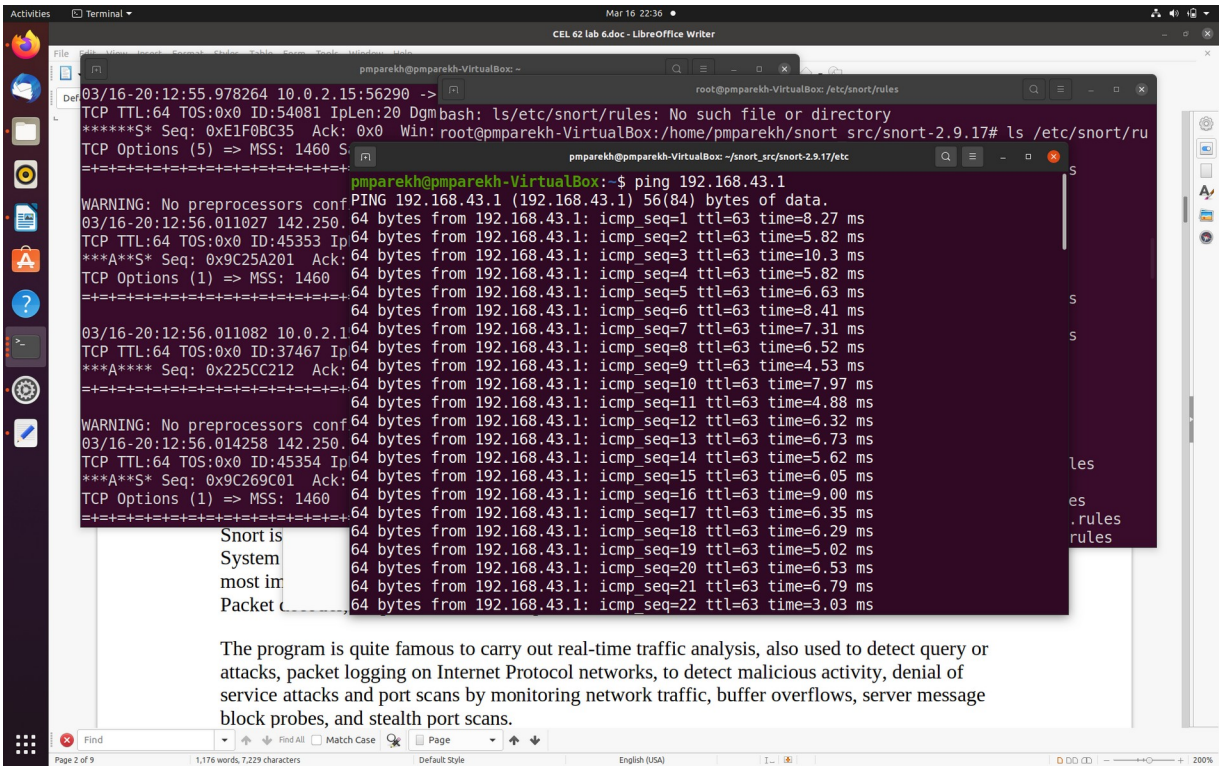
Writing and Adding a Snort Rule

Next, we are going to add a simple snort rule. You should add your own rules at /etc/snort/rules/local.rules. Add the following line into the local.rules file

alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)

Basically, this rule defines that an alert will be logged if an ICMP packet is found. The ICMP packet could be from any IP address and the rule ID is 1000001. e.g. Make sure to pick a SID greater 1000000 for your own rules.

To make the rule become effective, you need to restart the snort service by typing the following command.

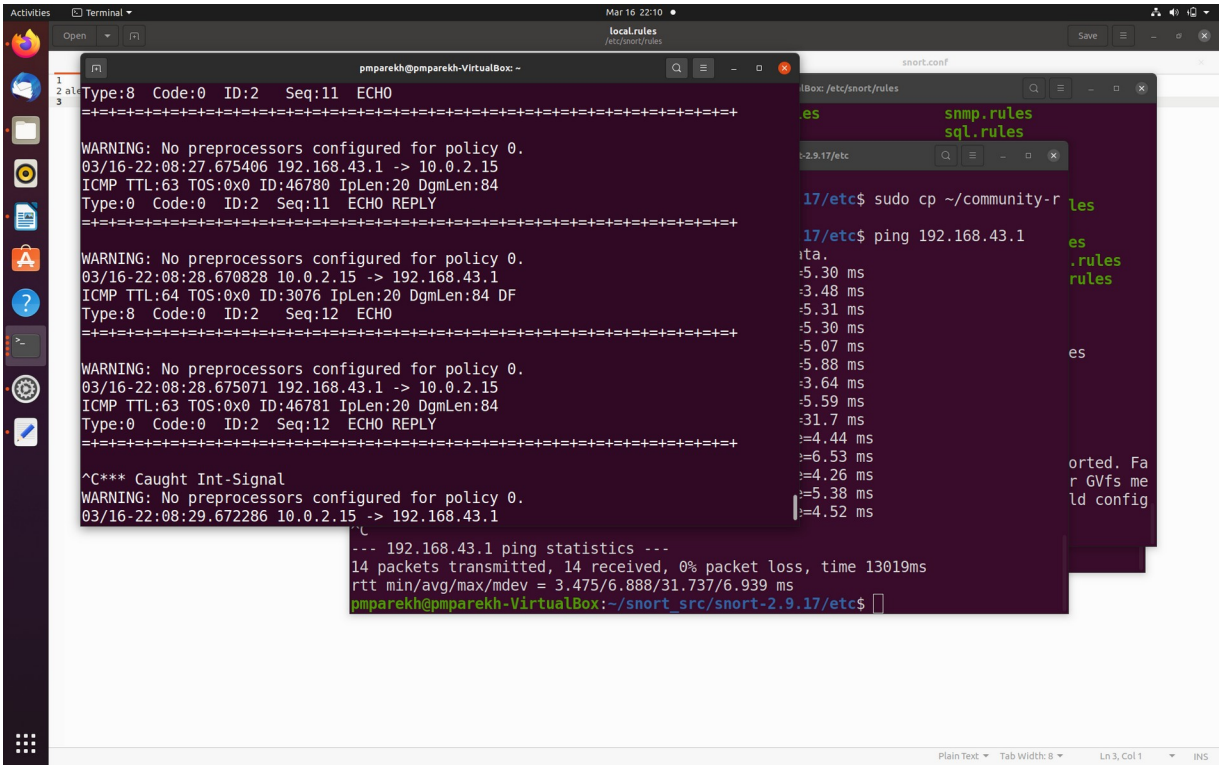


$ service snort restart

or

$ /etc/init.d/snort restart

Pinging from Ubuntu to Windows



Triggering an Alert for the New Rule

To trigger an alert for the new rule, you only need to send an ICMP message to the VM image where snort runs. First, you need to find the IP address of the VM by typing the following command.

$ ifconfig

For instance, the screenshot shows the execution result on my VM image, and the IP address is e.g. 172.16.108.242

After you have a terminal, you can just type the following command to send ping messages to the VM.

ping 172.16.108.242

After you send the ping messages, the alerts should be triggered and you can find the log messages in /var/log/snort/snort.log. However, the snort.log file will be binary format. You need to use a tool, called u2spewfoo, to read it. Observer terminal on screen with log where you can see that the SID is 1000001, and the alerts are generated by the ICMP messages.

Error no log directory

Assignments for Lab 1

1.Read the lab instructions above and finish all the tasks.

2.Answer the questions and justify your answers. Simple yes or no answer will not get any credits.

a. What is a zero-day attack? => A zero day attack means the developer doesn't have prior knowledge of the attack. A zero day is attack is very vulnerable since an attacker can exploit a vulnerability till it is found. This type of attack includes like SQL injections, buffer overflows, missing authorizations, broken algorithms.

b. Can Snort catch zero-day network attacks? If not, why not? If yes, how? => No, snort cannot catch zero-day network attacks. Since snort checks for the pre-defined rules for the zero-day attack and no developer can add all the rules for preventing the attack.

c. Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95%,and the probability that an alarm is an attack is 95%. What is the false alarm rate?

Ans c. => Here, we have 1 million connections which are 10,00,000. So number of attacks are 0.1% = 10^{-3}*10,00,000 = **1,000 attacks**. So no attacks are 99.9%*10,00,000 = **9,99,000 attacks**. Now we have a true positive rate of 95% so the number of alarms that are set by true attacks are 95%*1,000 = **950 alarms**. Therefore number of false alarms = 1,000 – 950 = **50**. Therefore the number of false alarm rate = (Number of false alarm/Total number of alarms not set) * 100 = (50/9,99,000) * 100 = **0.005%**.

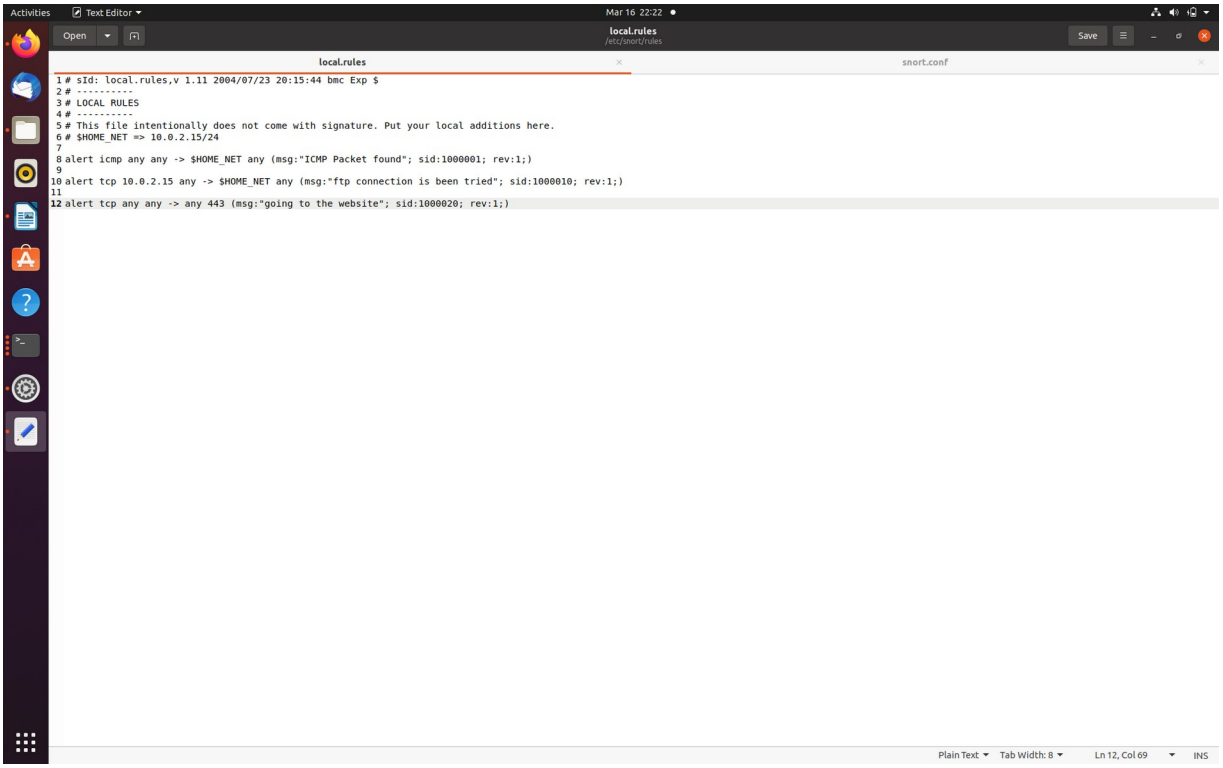
3.Write and add another snort rule and show me you trigger it.

a. The rule you added (from the rules file)

b. A description of how you triggered the alertc. The alert itself from the log file (after converting it to readable text)

Extra Credit (10pt):Write a rule that will fire when you browse to any site from the machine Snort is running on; it should look for any outbound TCP request to the site you have considered and alert on it.

Rules file



Conclusion -

After completing the above experiment, I have understood the following things -

1. A zero day attack can’t be stopped by SNORT

2. SNORT requires a lot of libraries to functions. One important being libpcap. This library helps in analyzing and sniffing TCP/IP traffic.

References -

1. https://www.youtube.com/watch?v=nSjtxIZgg8s

2. https://www.youtube.com/watch?v=2Yiyeu7TFbQ