International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

Detect Network Threat Using SNORT Intrusion Detection System

Nitin Verma

Dept. of Information Technology, USICT, Guru Gobind Singh Indraprastha University, Delhi, India

---

Abstract - *The general trend in a network company is a shift from "Intrusion Detection Systems (IDS) to Intrusion Prevention Systems (IPS)".and important and lots of sensitive data that can be misused data also information will be a leak that is a very critical situation to the company andit's all the employees to work company or office. Some of the available IDS tools Real-time analysis of several Internet attacks were done using SNORT, and Nmap to study the maliciousbehavior of our network. Intrusion Detection System is all the packets passing through the network and raises an alarm to generate this is an attempt to perform malicious activity. Snort is an open-source, freely available, and lightweight network intrusion detection system (NIDS) and that can capture all packets' details that passing through the networks, and alerts messages can be generated if anyone's packets match the signatures pattern then detects network threats.This soft work is used for Linux and Windows. In this work, we have to implemented and configure ids snort tools to detect network threats.*

Key Words: **Intrusion detection System, IDS, Signature based, Snort, Network threats IDS, Wireshark**

1. INTRODUCTION

Now a day's network security protect the data from the intruder. To protect the system web firewalls, encrypted data, and virtual private networks secure network infrastructure and communicate internet. An intrusion detection system (IDS) protects the data of the organization's host base network and detects malware activity, allowing IDS and administrators to take secure data and respond to these attacks.

IDS (intrusion detection system)[2] is a type of computer network security software. An An intrusion detection system aids in the detection of external and internal attacks carried out by users or hackers. The objective of this research is to look at an unusual link that our Intrusion Detection System identified using Snort. Now use Snort tools and configure them to detect network threats. This tool has the ability to collaborate and share information. The term "intrusion detection system" refers to software, hardware, or a mix of both that is used to detect intruder activities.

One of the most significant issues that all businesses face from time to time is network security[3]. There are many hackers attempting to breach the security of company or office networks, and some of them succeed in breaching security and leaking information. As a result, one of the most critical responsibilities for a firm to thrive is to secure its network." They utilise an Intrusion Detection System to make this easier and more efficient. This system helps collect information about any malicious packet that comes through a company's network[3]. Intrusion detection aids in the detection of both external and internal attacks carried out by users and hackers.

The goal of the project was to design and build an anomaly or behavioral-based Network Intrusion Detection System that could identify intrusions based on signature patterns as well as unusual new assaults. Snort to be Install Kali Linux, Ubuntu, window in a virtual machine and Configure Snort using commands. First, install snort and configure to use the install command. After successfully installed Snort, then need to install the rules and configure the file used for Snort. To display alert messages generated by Snort when capturing prospective intrusion actions. Then detect network threats from one network to another network.

Advantages of the Intrusion detection system

- An intrusion detection system (IDS) is a computer-based system that detects unauthorized access.
- Analysis of ongoing traffic, activity, transaction and behavior for anomalies.
- Network behavior to track any changes.

Disadvantages of the intrusion detection system

- Heavy processing.
- It is not fully safe from attacks.
- The intrusion detection system is time-consuming.

2. AIM AND OBJECTIVES

- It can monitor the traffic flow for any malicious-harmful activities of a network in real-time.
- They can prevent or overload bandwidth and Denial of Service (DoS) attacks.
- To create an intrusion detection system that can work with any operating system.

The project's goal was to "create and construct an Anomaly or Host-based Network Intrusion Detection System" that could identify intrusions based on behavioural patterns as well as unusual new assaults. Snort to be used Linux in a virtual machine and Configure Snort using commands. They

must first install the required applications and libraries before installing snort. After successfully installed Snort, then need to install the rules and configure the file used for Snort. The Snort configuration system snort.conf files are now located in this path /etc/snort, to make the changes it works well on our system[1]. To display alert messages generated by Snort when capturing prospective intrusion actions. Then detect network threats from one network to another network.

3. LITERATURE REVIEW

Snort[1] is a lightweight intrusion detection tool it is free to open source network IDS & IPS. First release 1998 (Martin Roesch, Founder and former CTO of Source fires). "Snort is created by Cisco, and stable release 2.96.1/August 2, 2020 is written in C," according to the license, which is GPLv2+. It produces log files and analyses packets as they pass through network traffic[4]. Snort rules detect harmful behaviour and send out alarm messages. Users write snort rules in a text file format that is connected to a snort.conf file that contains all of the snort configurations as well as alert details. There are a few instructions that may be used to start the snort tools so that they can analyse and monitor network traffic activity.

4. COMPONENTS OF A SNORT-BASED IDS

i. **Packet Decoder**: - The packet decoder collects packets from multiple network interfaces and prepares them for pre-processing or transmission to the detection engine. One of the interfaces, for example, may be Ethernet[1].

ii. **Preprocessors**: - Preprocessors are also used for packet defragmentation. Snort preprocessors are components or plug-ins that may be used to organise or change data packets before the detection engine conducts an operation to see if the packet is being utilised by an intruder[2]. Some preprocessors will additionally emit alerts if anomalies in packet headers are detected. Preprocessors are critical for any IDS since they prepare data packets for the detection engine's rules to analyse[3].

iii. **Detection Engine**: **-** Snort's detection engine is its most essential component. Its purpose is to see whether there is any intrusion activity in data packets. For various versions of Snort, the detection engine functions in different ways[3]. The following elements influence the detecting engine's load:
- The amount of rules there are.
- The processing power of the computer on which Snort is installed.
- The speed of the Snort machine's internal bus.
- Make a network load.

iv. **Logging and Alerting System**: - Based on what the detection engine detects inside the packet, it can be used to log activities or generate an alarm.[3].

v. **Output Modules**: - Depending on how you want to store Snort's logging and alerting system output, output modules or plug-ins can perform various tasks.

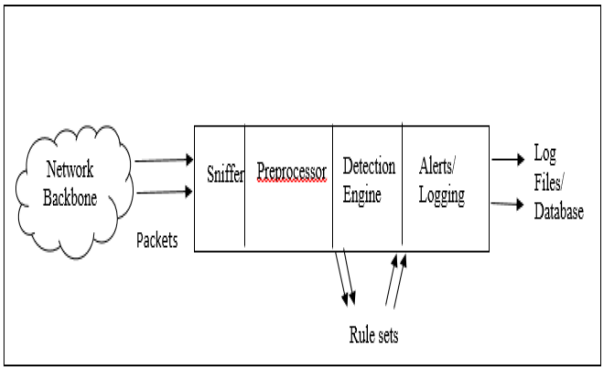


Fig 1: Snort Architecture

5. METHODOLOGY

The two types of IDS techniques are:

i. **Signature-based intrusion detection technique**: Signature-based intrusion detection technique to detect new patterns, their network traffic, and the anti-virus software to detected the digital signature pattern and they knew attacks for no pattern is available[6]. Misuse detection techniques are automatically created and it's complicated and manually done the system and they should be sent notification to be right authorities.

Advantages of Signature-based intrusion detection technique

- They Detect known attacks.
- They know which attack at the time of detection.

Disadvantages of Signature-based intrusion detection technique

- Signature files must be up to date.
- They can only detect known attacks.

ii. **Anomaly-based intrusion detection technique:** An Anomaly-based intrusion detection system technique of their network and computer-based intrusions detection system will be an unwanted activity they are normal[6]. Some digital signatures or some patterns are they detect any harmful

activity to be the normal system they signature-based systems detect attacks for previously has been a crested signature.

Advantages of Anomaly-based intrusion detection system

- They will not require constantly keeping up on the hacking technique.
- It's more efficient as compared to signature-based.
- They are a chance of detecting unknown attacks.

Disadvantages of Anomaly-based intrusion detection system

- They are a lack of specific information on a possible attack
- Anomaly implies unusual activity.

6. CONFIGURATION AND IMPLEMENTATION OF SNORT

6.1 Requirements

- Operating system: Kali Linux, Ubuntu, and window (Virtual Machine).
- RAM: Minimum: 2GB.
- Hard disk Space: Minimum 40 GB.
- Install Apache Web server.
- Install and protect MySQL database.
- Install PHP Hypertext Preprocessor.
- Install Snort.
- Install Barnyard2.
- Install ADOdb (Active Data Object Data Base).
- Install BASE (Basic Analysis and Security Engine).

First Install VMware to install Ubuntu as per requirement and configure them and install another machine to attack those machine.

There is install the Snort tool it can use command: **apt-get install snort.** Then setup and configure: **Snort –h (**Show all options**)**. To verify the Snort version, type in **snort -V** and hit Enter.

```
root@ubuntu:/home/nitin/Desktop# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

Snap 1: Show snort version

Next, we want to configure our HOME_NET value: the network we will be protecting. First, enter **ifconfig** the command to know the interface ip address.

```
root@ubuntu:/home/nitin/Desktop# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.159.128  netmask 255.255.255.0  broadcast 192.168.159.255
       inet6 fe80::4114:3421:c4c:6164  prefixlen 64  scopeid 0x20<link>
       ether 00:0c:29:7f:f1:c0  txqueuelen 1000  (Ethernet)
       RX packets 13957  bytes 20531799 (20.5 MB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 1867  bytes 135372 (135.3 KB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Snap 2: Interface

The Address to be your actual class C subnet. Currently, it should be *192.168.159.0/24*. They are changing any IP address to the server so leave the 0/24 on the end. Snort can use a Snort configuration file at the start-up time. The configuration file on this pathname snort.conf to snort distribution and the home net IP address.

Snort IDS tools have their own predefined rules, which we can do by detecting intrusion in them. But by disabling all these rules, and create my own IDS rules.

```
4150 Snort rules read
    3476 detection rules
    0 decoder rules
    0 preprocessor rules
3476 Option Chains linked into 290 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Snap 3: predefined rules

Here we are telling Snort to test (**-T**) the configuration file (**-c** points to its location) on the **eth0** interface (enter your interface value if it's different). This will produce a lot of output. To see the "0 Snort rules read". **sudo gedit /etc/snort/snort.conf**

```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
0 Snort rules read
    0 detection rules
    0 decoder rules
    0 preprocessor rules
0 Option Chains linked into 0 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Snap 4: Disable all rules

Let's create our first ICMP test rule. This rule will generate an alert message whenever Snort detects an ICMP ping request or reply message. Open the local.rules file in a texteditor as root with the following command: **sudo gedit /etc/snort/rules/local.rules alert [write which of attack] any any -> $HOME_NET any (msg:"Type any message"; sid:100000 rev:1; classtype: if any)**

6.2 Rule header

alert – Action on the rules. Based on the situation, produce an alert message.

any – Snort will check for all sources, including IP addresses.

any – The location of the source port. All ports will be examined by Snort.

-> – This Symbol is source address to destination address.

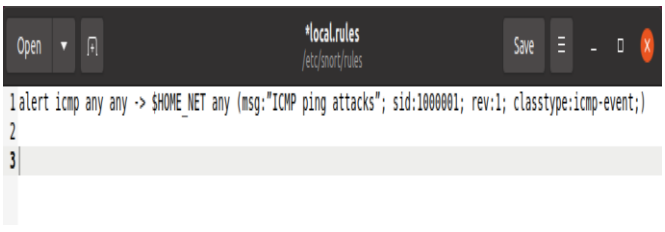
$HOME_NET – IP address of the destination.

any – The port of destination. All of the protected network's ports.

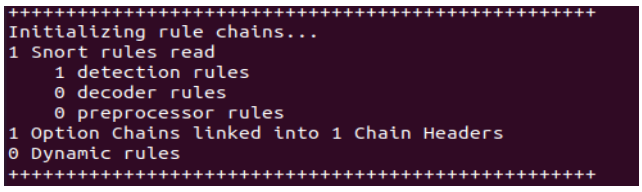
6.3 Rule Options

Msg-"ICMP ping attacks" – Snort will add this message as a rule in the alert. Snort rule IDs up to 1,000,000 are reserved, so start with 1000001. (you may use any number, as greater than 1,000,000).

rev:1 – Number of revisions. This option makes rule maintenance easy. classtype: icmp-event – Labels the rule as a "icmp-event," one of Snort's preset categories. This option aids in the arrangement of rules.



Snap 5: Create new rules



Snap 6: show new rules

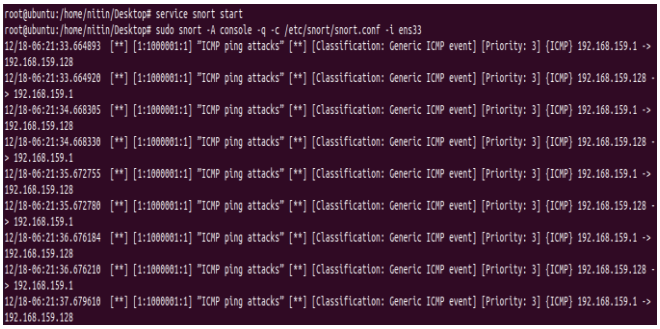
The snort.conf configuration file, which is provided in the snort package, can be used by Snort[14]. Now Start Snort service to intrusion detection system services is activated following this command **service snort start.** Then set the alert mode to detect all threats on our system and configuration file to save directory now following this command: **sudo snort -A console -q -c /etc/snort/snort.conf -i ens33.**

-q: Logs and alerts banner don't show.

-A: This use in alert mode and to print the output to the console.

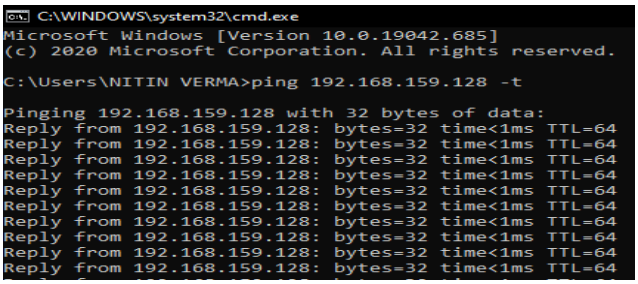
-i: It represents the network interface for Ethernet those used "ens33" to Ip address.

-c: It's located config file



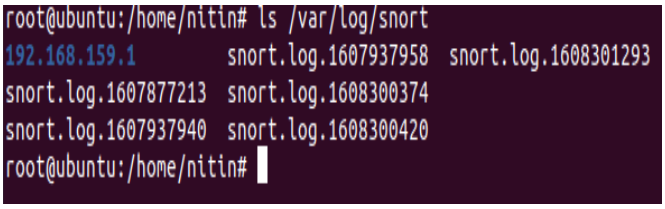
Snap 7: Show alert message

There is used to another attack machine continuously ping requests and generate ICMPand check your system they can detect threats. Following this ping request command **$ping 192.168.159.128 –t**
-t: unlimited time ping request



Snap 8: Attack another machine

There Snort tools detect the threats to alerts mode and protect your system. Classification is a misc activity for ICMP. The following command to do the listing of the Snort log directory: **ls /var/log/snort**

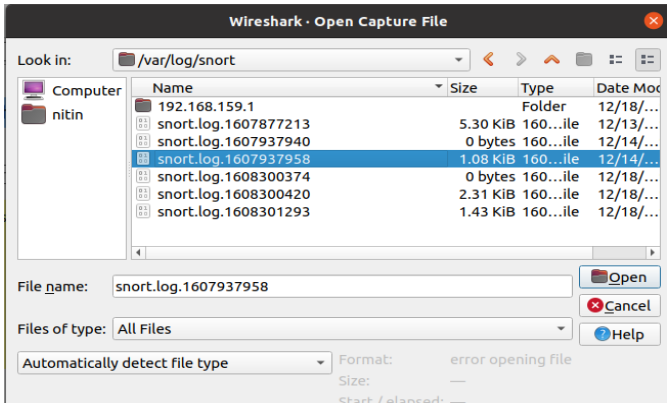


Snap 9: Check snort log files

The IP address that you see is the source IP for the alert we just saw for our FTP rule. It is a directory. Let's see what's inside:

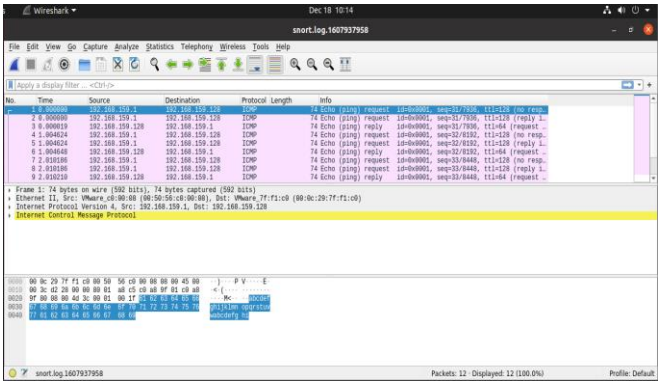
sudo ls /var/log/snort/192.168.159.1

We get the same information as we saw in the console output with some additional details. We can use Wireshark tools it is a most popular network protocol analyzer, to passive attack check. Enter **sudo wireshark** to start the program.



Snap 10: Wireshark

A lot more information here to check passive attack. Now we can look at the contents of each packet.



Snap 11: Show Attacks packet

8. CONCLUSION

In this work, we have designed and implemented a real-time Intrusion detection system withthe help of the integration of Snort (A signature-based system and Anomaly-based system) and proposes an architecture to enhance the efficiency of Snort IDS. This of our project work willbe the display of all network traffic packets which match the snort defined rule by the administrator. The information includes Source, Destination, unique Alert generated, Date, andTimestamp of when the packet was received[5] or net. Snort is a lightweight IDS, which uses a bunch of build-in rules and user-customized rules to prevent a prospective intruder from intruding in a network system.

This work discussed the installation procedure for Snort as well as other products that work with Snort, components of Snort, and most frequently used functions. Finally, we gave a test in the Kali Linux system about analyzing alerts generated by Snort based on some specific rules. In the future, we will integrate the proposed design into the Snort tool and evaluate it to achieve a better detection rate with fewer false (negative) alarms[6].

REFERENCES

[1] Aaliya Tasneem, A. K. (2018). Intrusion Detection Prevention System using SNORT. International Journal of Computer Applications (0975 – 8887), Volume 181.

[2] Deepak Kumar Singh, M. J. (2016). An approach for Anomaly based Intrusion System using SNORT. International Journal of Scientific & Engineering Research, Volume 4.

[3] Hamsaveni, R. (2020). AN IMPLEMENTAION OF SNORT BASED INTRUSION DETECTION SYSTEM USING WIRELESS SENSOR NETWORK. International Research Journal of Modernization in Engineering Technology and Science, Volume:02/Issue:12, 12-22.

[4] LIN Ying, Z. Y.-J. (2010). The Design and Implementation of Host-based Intrusion Detection System. IEEE.

[5] Monowar H. Bhuyan, D. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. IEEE Communications Surveys & Tutorials, 1-34.