Don Bosco Institute of Technology, Mumbai 400070 Department of Information Technology

Experiment No. : 12

Name: Swasti Jain
Batch: B
Roll No: 24

Title: SNORT and studying the logs.

Problem Definition : Study network security by installing an IDS, SNORT and study the logs.

Prerequisite : IDS **Theory :**

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors' ' and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.[1] IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

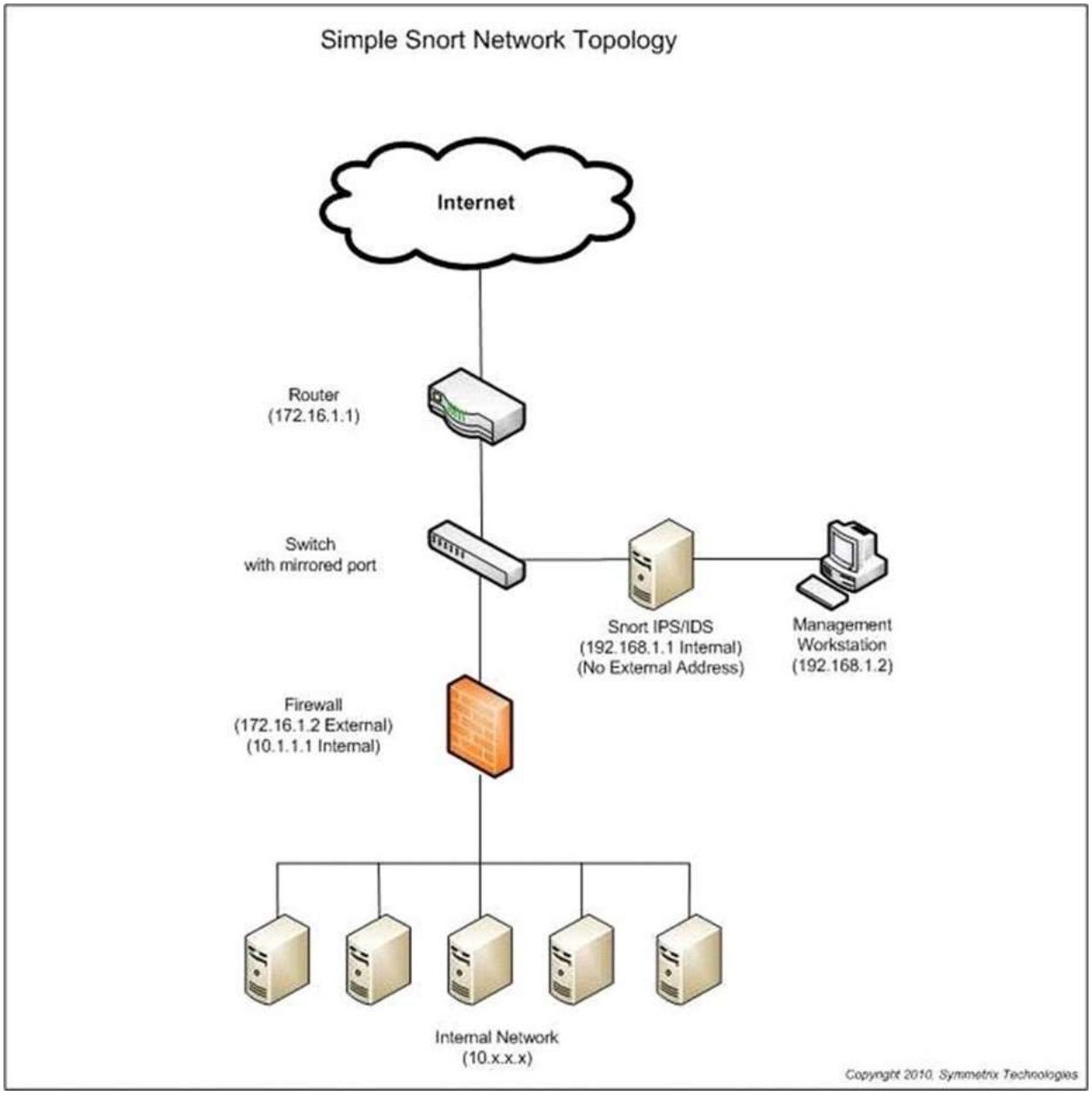
SNORT

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998. Snort is now developed by Sourcefire, of which Roesch is the founder and CTO. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time".

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified



Procedure/Algorithm : Snort Installation

Step 1: Update the system

First, update and upgrade your Ubuntu system
.sudo apt update
.sudo apt upgrade

Step 2: Install Required Dependencies

Ubuntu's default repository has a snort package. The snort package available there is the old version. To install Snort 3, we have to build from the source. Before installing Snort 3, we need to install the prerequisite and required libraries. Install Snort 3 dependencies packages with the following command:

command:

sudo apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdnet-dev libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev

After dependencies are installed, created a directory where you compile and kept source files for Snort with the following command

Command:

mkdir snort-source-files cd
snort-source-filesz

Then, download and install the latest version of the Snort Data Acquisition library (LibDAQ). For installing LibDAQ we'll need to build and install it from the source with the following command.

Command:

git clone https://github.com/snort3/libdaq.git cd
libdaq
./bootstrap
./configure
Make
make install

The next dependency is Tcmalloc, which will optimize memory allocation and provide better memory usage. Install Tcmalloc with the following command.

Command:

cd ../ wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.9/gperftool s-2.9.tar.gz tar xzf gperftools-2.9.tar.gz cd gperftools-2.9/ ./configure make make install

Step 3: Install Snort 3 on Ubuntu 20.04

After dependencies are set up, we are going to download and install Snort 3 on Ubuntu 20.04. 01. Clone Snort 3 official GitHub repository.

Command:

cd ../ git clone git://github.com/snortadmin/snort3.git

02. Change the directory to Snort3

Command

cd snort3/

03. From there configure and enable tcmalloc with the following command.

Command:

./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc

04. Navigate to build directory and compile and install Snort 3 using make and makeinstall with the following command.

Command:

cd build
make
make install

05. When the installation is done, update shared libraries.

Command:

sudo ldconfig

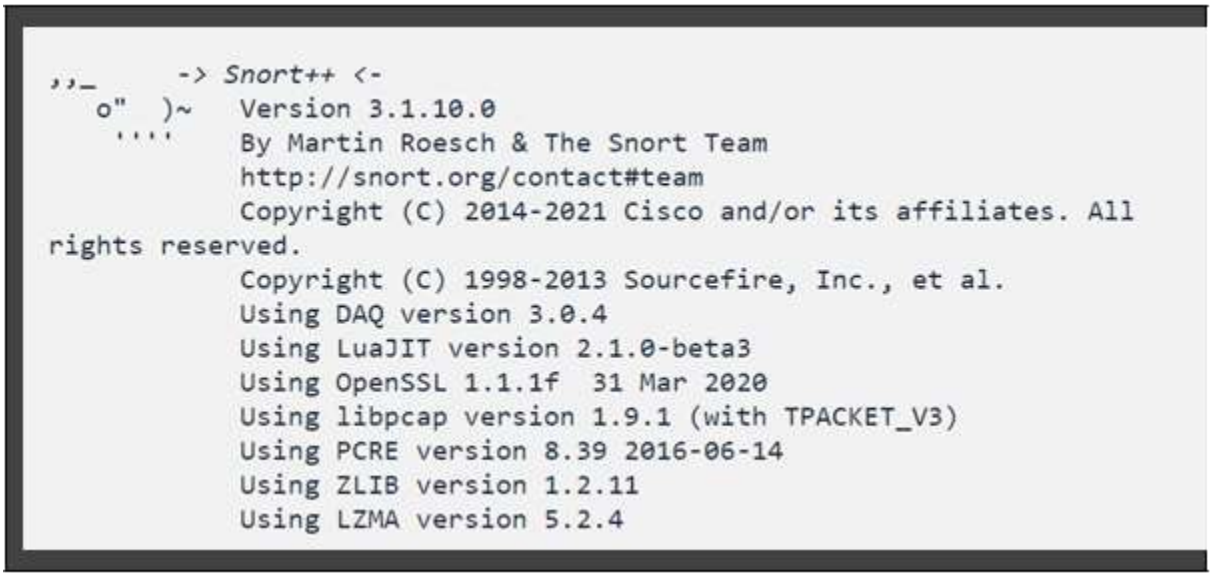
Snort by default is installed to /usr/local/bin/snort directory, it is good practice to create a symbolic link for /usr/sbin/snort

Command:

sudo ln -s /usr/local/bin/snort /usr/sbin/snort

06. Verify Snort 3 installation

Command:
snort -V Output:



Therefore, Snort 3 is installed successfully.

Step 4 : Running Snort as a Service

If you are going to run Snort as a service daemon in the background, it is also possible to create a systemd service unit for Snort. It is prudent to run it as a non-privileged system user. Create a non-login system user account

Command:
sudo useradd -r -s /usr/sbin/nologin -M -c SNORT_IDS snort

Then, create a systemd service unit for Snort to be run as a snort user. Adjust and match to your network interface.

Command:
sudo nano /etc/systemd/system/snort3.service Paste

the following configuration.

[Unit] Description=Snort 3 NIDS Daemon After=syslog.target network.target [Service] Type=simple ExecStart=/usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l /var/log/snort -D -i eht0 -m 0x1b -u snort -g snort [Install] WantedBy=multi-user.target

Reload the systemd configuration.

Command:
sudo systemctl daemon-reload

Set the ownership and permissions on the log file.

Command:
sudo chmod -R 5775 /var/log/snort sudo chown -R snort:snort /var/log/snort Start and

enable Snort to run on the system boot:

Command:
sudo systemctl enable --now snort3

Check the service status to confirm if it is running.

Command:
sudo systemctl status snort3

Output:

```
● snort3.service - Snort 3 NIDS Daemon
     Loaded: loaded (/etc/systemd/system/snort3.service; enabled;
vendor preset: enabled)
     Active: active (running) since Sat 2021-09-18 12:44:32 UTC; 6s ago
   Main PID: 182886 (snort)
      Tasks: 2 (limit: 1071)
     Memory: 62.6M
     CGroup: /system.slice/snort3.service
             └─182886 /usr/local/bin/snort -c
/usr/local/etc/snort/snort.lua -s 65535 -k none >
 Sep 18 12:44:32 li72-186 systemd[1]: Started Snort 3 NIDS Daemon.
```

Results : In this experiment we learnt to install the Snort 3 network intrusion detection system on Ubuntu 20.04.

References : https://upcloud.com/resources/tutorials/install-snort-ubuntu
https://linuxopsys.com/topics/install-snort-on-ubuntu