

Final Year B. Tech., Sem VII 2022-23
Cryptography And Network Security

Lab PRN : 2019BTECS00029

Name : Harshal Kodgire

Batch: B1

Assignment: 16

Title of assignment: Installation and Testing of Snort

Aim : To test and run snort

Theory:

SNORT is a network based intrusion detection system which is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software. It can also be used as a packet sniffer to monitor the system in real time. The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system. It is based on library packet capture tool. The rules are fairly easy to create and implement and it can be deployed in any kind of operating system and any kind of network environment. The main reason of the popularity of this IDS over others is that it is a free-to-use software and also open source because of which any user can be able to use it as the way he wants.

Features:

- **Real-time traffic monitor**
- **Packet logging**
- **Analysis of protocol**

- **Content matching**
- **OS fingerprinting**
- **Can be installed in any network environment.**
- **Creates logs**
- **Open Source**
- **Rules are easy to implement**

Installation of snort:

```
prathmesh@prathmesh-G3-3500:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 70:b5:e8:a7:c2:3e brd ff:ff:ff:ff:ff:ff
3: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether a8:7e:ea:99:8f:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.105/24 brd 192.168.233.255 scope global dynamic noprefixroute wlp0s20f3
        valid_lft 2493sec preferred_lft 2493sec
    inet6 2401:4900:5297:2993:59a6:ac33:e806:b23b/64 scope global temporary deprecated dynamic
        valid_lft 2518sec preferred_lft 0sec
    inet6 2401:4900:5297:2993:eca5:1d6d:8dfc:7917/64 scope global deprecated dynamic mngtmpaddr noprefixroute
        valid_lft 2518sec preferred_lft 0sec
    inet6 2409:4042:259f:bf5f:630d:6331:3fb4:be9d/64 scope global temporary dynamic
        valid_lft 3492sec preferred_lft 3492sec
    inet6 2409:4042:259f:bf5f:c08c:fd55:fe17:8d5c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 3492sec preferred_lft 3492sec
    inet6 fe80::afc9:3f28:6fc4:8be5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
prathmesh@prathmesh-G3-3500:~$
```

This value is usually "eth0", but this may be inappropriate in some network environments; for a dialup connection "ppp0" might be more appropriate (see the output of `/sbin/ifconfig`).

It is also not uncommon to use an interface with no IP address configured in promiscuous mode. For such cases, select the interface in this system that is physically connected to the network that should be inspected, enable promiscuous mode later on and make sure that the network traffic is sent to this interface (either connected to a "port mirroring/spanning" port in a switch, to a hub, or to a tap).

Interface(s) which Snort should listen on:

<Ok>

Plain Text ▼ Tab Width: 8 ▼ Ln 51, Col 30 ▼ INS

```
prathmesh@prathmesh-G3-3500: ~  
prathmesh@prathmesh-G3-3500: ~$ sudo cp /usr/share/doc/snort3-source-files/snort3 sudo gedit /etc/snort/snort.conf  
[sudo] password for prathmesh:  
  
(gedit:33714): Tepl-WARNING **: 15:08:11.331: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform.  
In the latter case, you should configure Tepl with --disable-gvfs-metadata.  
prathmesh@prathmesh-G3-3500: ~$ snort-source-files/snort3 $ cd cd  
bash: cd: cd: No such file or directory  
prathmesh@prathmesh-G3-3500: ~$ snort-source-files/snort3 $ cd ..  
prathmesh@prathmesh-G3-3500: ~$ snort-source-files $ cd ..  
prathmesh@prathmesh-G3-3500: ~$ mkdir /usr/local/etc/rules  
mkdir cannot create directory '/usr/local/etc/rules': Permission denied  
prathmesh@prathmesh-G3-3500: ~$ sudo mkdir /usr/local/etc/rules  
prathmesh@prathmesh-G3-3500: ~$ wget https://www.snort.org/downloads/community/snort3-community-rules.tar.gz  
2022-11-21 15:08:56 - https://www.snort.org/downloads/community/snort3-community-rules.tar.gz  
Resolving www.snort.org (www.snort.org)... 2006:470d:90d3:f255::ecad:b612:8a09, 104.18.139.9, 104.18.139.9  
Connecting to www.snort.org (www.snort.org) [2006:470d:90d3:f255::ecad:b612:8a09]:443... connected.  
HTTP request sent, awaiting response... 200 Found  
https://www.snort.org/downloads/community/production/release_files/files/000/028/918/original/snort3-community-rules.tar.gz?zX=Anz-AloorithmAwSd-HMAC-SHA256&X=Anz-Credential=AKIAU7AKSTH3QBPAPZP
```

```

prathmesh@prathmesh-G3-3500:~$ ifconfig -a
enp4s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 70:b5:e8:a7:c2:3e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1012 bytes 97626 (97.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1012 bytes 97626 (97.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.233.105 netmask 255.255.255.0 broadcast 192.168.233.255
    inet6 2401:4900:5297:2993:59a6:ac33:e806:b23b prefixlen 64 scopeid 0x0<global>
    inet6 2401:4900:5297:2993:eca5:1d6d:8dfc:7917 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::afc9:3f28:6fc4:8be5 prefixlen 64 scopeid 0x20<link>
    inet6 2409:4042:259f:bf5f:c08c:fd55:fe17:8d5c prefixlen 64 scopeid 0x0<global>
    inet6 2409:4042:259f:bf5f:630d:6331:3fb4:be9d prefixlen 64 scopeid 0x0<global>
    ether a8:7e:ea:99:8f:31 txqueuelen 1000 (Ethernet)
    RX packets 19365 bytes 21359173 (21.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12153 bytes 2033602 (2.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

prathmesh@prathmesh-G3-3500:~$

```

Testing of snort: Ip 192.168.16.3 is trying to ping the host 192.168.16.105 and it get detected on snort

