

Assignment 4

Study Of Snort – An Intrusion Tool

AIM

Configure and demonstrate use of network intrusion tools such as Snort security perspective.

OBJECTIVE:

Study of any intrusion software and use its implementation features.

THEORY

IDS Stands for Intrusion Detection System. The techniques and methods on which an IDS is founded on are used to monitor and reveal malicious activities both on the host and network level. Once the said activities occur then an alert is issued to aware every one of the attack. It can be hardware or software or a combination of both; depends on the requirement. An IDS uses both signature or anomaly based technique together or separately; again depending on requirement. Your network topology determines where to add intrusion detection systems. Whether it should be positioned at one or more places depends on if you want to track internal threat or external threat. For instance, if you want to protect yourself from external traffic then you should place an IDS at the router and if you want to protect the inner network then place the IDS on every network segment.

Snort is an open source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort consists of the following components

- Packet Decoder
- Pre-processors
- Detection Engine
- Logging and Alerting System
- Output Modules

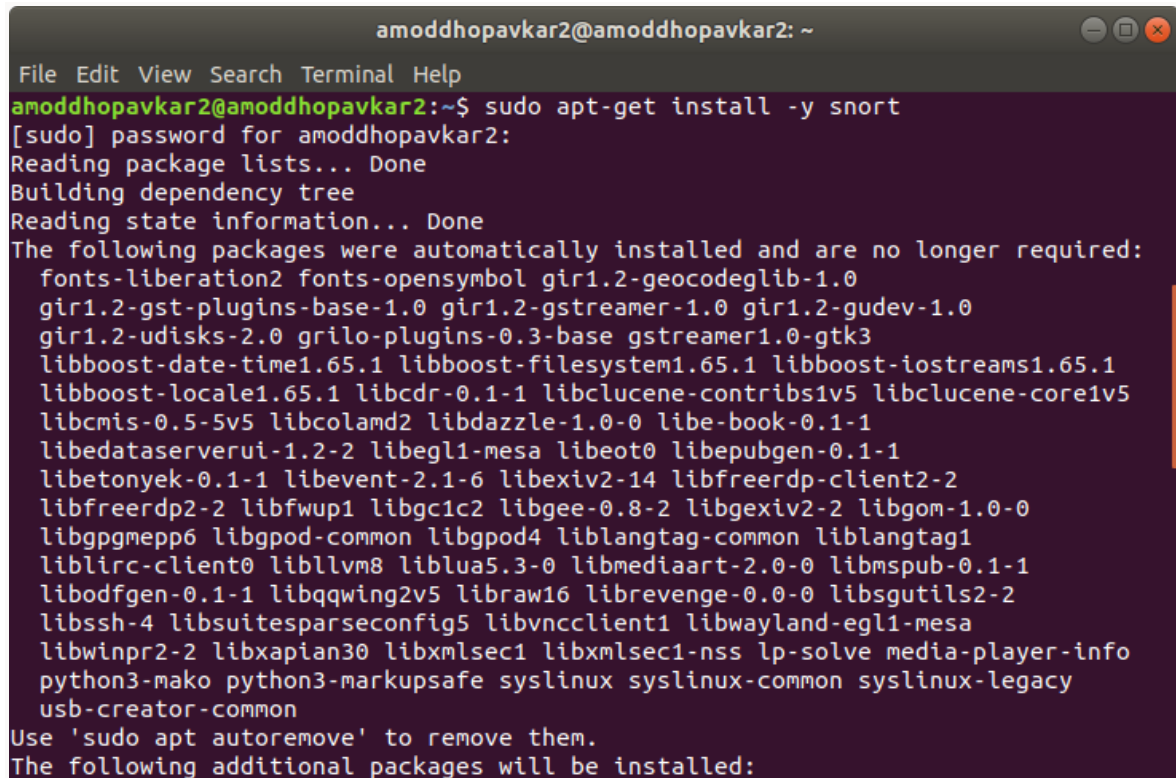
Platforms on which Snort runs

Snort runs on most UNIX and various windows. It requires GTK+, GTK6, libpcap and other libraries in order to run.

- UNIX
Applet, MAC, BEOS, JBM, AIX, BSD open etc.
- LINUX
Mandrake LINUX, Red Hat, SUSE LINUX etc.
- WINDOWS
Windows server 2003/XP/2000/NT/7/10

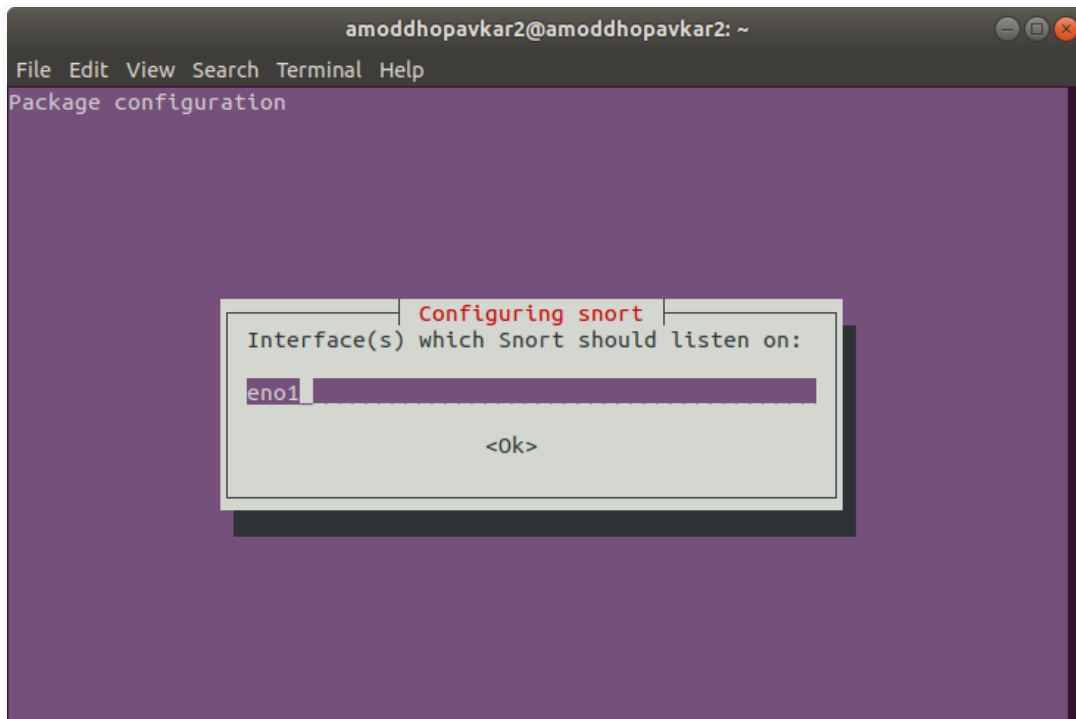
Installing Snort

- Snort is installed using the following command
`sudo apt-get install snort`

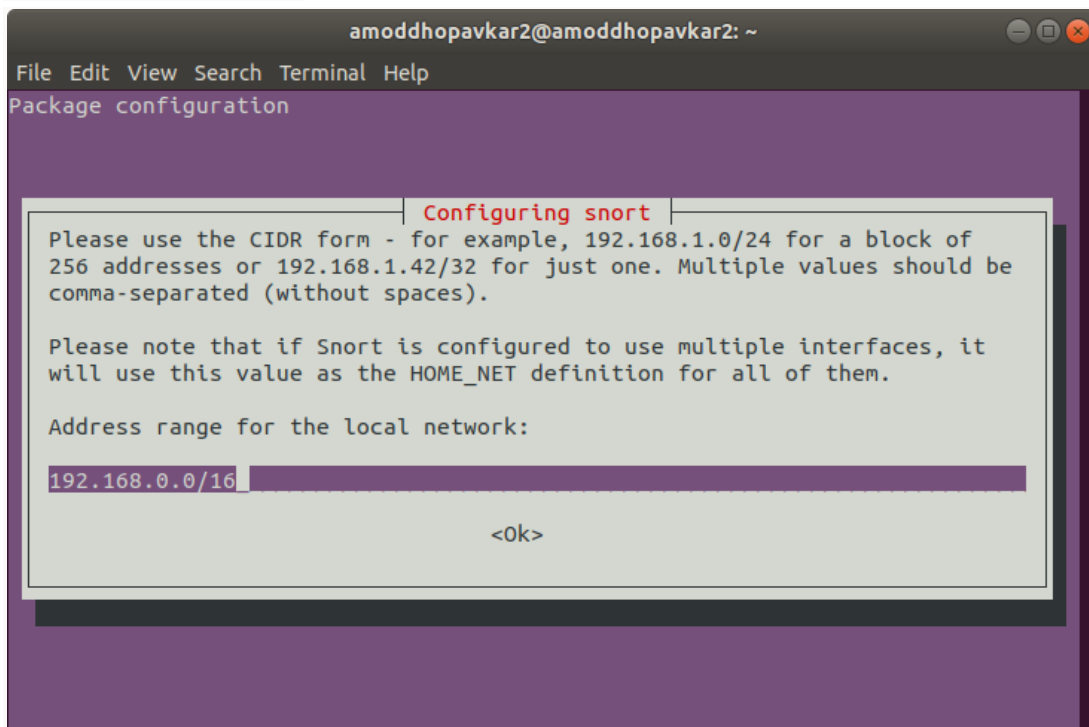


```
amoddhopavkar2@amoddhopavkar2: ~  
File Edit View Search Terminal Help  
amoddhopavkar2@amoddhopavkar2:~$ sudo apt-get install -y snort  
[sudo] password for amoddhopavkar2:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  fonts-liberation2 fonts-opensymbol gir1.2-geocodeglib-1.0  
  gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0  
  gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3  
  libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1  
  libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5  
  libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1  
  libedataserverui-1.2-2 libegl1-mesa libeot0 libepubgen-0.1-1  
  libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2  
  libfreerdp2-2 libfwup1 libgc1c2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0  
  libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1  
  liblirc-client0 libllvm8 liblua5.3-0 libmediaart-2.0-0 libmsspub-0.1-1  
  libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2  
  libssh-4 libsuitesparseconfig5 libvncclient1 libwayland-egl1-mesa  
  libwinpr2-2 libxapian30 libxmlsec1 libxmlsec1-nss lp-solve media-player-info  
  python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy  
  usb-creator-common  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:
```

- Once the installation starts, it will ask you the interface that we previously checked. Give its name here and press enter.



- Then it will ask you about your network IP. Here, you can either provide a single IP or the range of IPs



- As the snort is installed, open the configuration file using nano or any text editor to make some changes inside.

```
sudo nano /etc/snort/snort.conf
```

- Scroll down the text file near line number 45 to specify your network for protection as shown in the given image.

```
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.1.21

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

- Now run given below command to enable IDS mode of snort .

```
sudo snort -A console -i ens33 -c /etc/snort/snort.conf
```

- Once the snort is installed and configured, we can start making changes to its rules as per our own requirement and desire

```

+-----+
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x7fbe18885700 (4934)
Decoding Ethernet

--== Initialization Complete ==--

    ,,-
    o" )~
    '---

    -*> Snort! <*-
    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 1.8.1
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.2.11

    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
    Preprocessor Object: SF_SDF Version 1.1 <Build 1>
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
    Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
    Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
    Preprocessor Object: SF_SIP Version 1.1 <Build 1>
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>
    Preprocessor Object: SF_POP Version 1.0 <Build 1>
    Compiling packet processor (pid 4934)

```

- `cd /etc/snort/rules ls -la`

```

amoddhopavkar2@amoddhopavkar2: /etc/snort/rules
File Edit View Search Terminal Help
amoddhopavkar2@amoddhopavkar2:~$ cd /etc/snort/rules
amoddhopavkar2@amoddhopavkar2:/etc/snort/rules$ ls -la
total 1608
drwxr-xr-x 2 root root 4096 Sep 21 02:35 .
drwxr-xr-x 3 root root 4096 Sep 21 02:40 ..
-rw-r--r-- 1 root root 5520 Apr 3 2018 attack-responses.rules
-rw-r--r-- 1 root root 17898 Apr 3 2018 backdoor.rules
-rw-r--r-- 1 root root 3862 Apr 3 2018 bad-traffic.rules
-rw-r--r-- 1 root root 7994 Apr 3 2018 chat.rules
-rw-r--r-- 1 root root 12759 Apr 3 2018 community-bot.rules
-rw-r--r-- 1 root root 1223 Apr 3 2018 community-deleted.rules
-rw-r--r-- 1 root root 2042 Apr 3 2018 community-dos.rules
-rw-r--r-- 1 root root 2176 Apr 3 2018 community-exploit.rules
-rw-r--r-- 1 root root 249 Apr 3 2018 community-ftp.rules
-rw-r--r-- 1 root root 1376 Apr 3 2018 community-game.rules
-rw-r--r-- 1 root root 689 Apr 3 2018 community-icmp.rules
-rw-r--r-- 1 root root 2777 Apr 3 2018 community-inap.rules
-rw-r--r-- 1 root root 948 Apr 3 2018 community-inappropriate.rules
-rw-r--r-- 1 root root 257 Apr 3 2018 community-mail-client.rules
-rw-r--r-- 1 root root 7837 Apr 3 2018 community-misc.rules
-rw-r--r-- 1 root root 621 Apr 3 2018 community-nntp.rules
-rw-r--r-- 1 root root 775 Apr 3 2018 community-oracle.rules
-rw-r--r-- 1 root root 1621 Apr 3 2018 community-policy.rules
-rw-r--r-- 1 root root 3551 Apr 3 2018 community-sip.rules
-rw-r--r-- 1 root root 2722 Apr 3 2018 community-smtp.rules
-rw-r--r-- 1 root root 4063 Apr 3 2018 community-sql-injection.rules
-rw-r--r-- 1 root root 3742 Apr 3 2018 community-virus.rules
-rw-r--r-- 1 root root 2406 Apr 3 2018 community-web-attacks.rules
-rw-r--r-- 1 root root 5128 Apr 3 2018 community-web-cgi.rules
-rw-r--r-- 1 root root 4589 Apr 3 2018 community-web-client.rules
-rw-r--r-- 1 root root 254 Apr 3 2018 community-web-dos.rules
-rw-r--r-- 1 root root 1473 Apr 3 2018 community-web-its.rules
-rw-r--r-- 1 root root 68917 Apr 3 2018 community-web-misc.rules
-rw-r--r-- 1 root root 163259 Apr 3 2018 community-web-php.rules
-rw-r--r-- 1 root root 7646 Apr 3 2018 ddos.rules
-rw-r--r-- 1 root root 64313 Apr 3 2018 deleted.rules
-rw-r--r-- 1 root root 6743 Apr 3 2018 dns.rules
-rw-r--r-- 1 root root 6296 Apr 3 2018 dos.rules

```

- To check whether the Snort is logging any alerts as proposed, add a detection rule alert on IP packets in the “local.rules file”
 - `echo "" > icmp-info.rules`
 - `cat icmp-info.rules`

```

root@ubuntu:/etc/snort/rules# echo "" > icmp-info.rules
root@ubuntu:/etc/snort/rules# cat icmp-info.rules

root@ubuntu:/etc/snort/rules# echo "" > icmp-info.rules
root@ubuntu:/etc/snort/rules# cat icmp-info.rules

```

- Sample Rule
 - `alert icmp any any -> 192.168.1.21 any (msg: "ICMP Packet found"; sid:10000001;)`
- On Intrusion snort will output

```

alert icmp any any -> 192.168.1.21 any (msg: "ICMP Packet found"; sid:10000001; )

```

- Now we will apply rules on port 21, 22 and 80. This way, whenever a suspicious packet is sent to these ports, we will be notified. Following are the rules to apply to achieve the said
 - alert tcp any any -> any 21 (msg: "FTP Packet found"; sid:10000002;)
 - alert tcp any any -> any 22 (msg: "SSH Packet found"; sid:10000003;)
 - alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000004;)

```
alert tcp any any -> any 21 (msg: "FTP Packet found"; sid:10000002; )
alert tcp any any -> any 22 (msg: "SSH Packet found"; sid:10000003; )
alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000004; )
```

CONCLUSION

Hence we studied the network intrusion detection system known as Snort and showed its demonstration.