

IDS & IPS using Snort



Instructor

Dr. Debasis Das
Associate Professor, CSE
IIT Jodhpur

Co-taught by

Ayanabha Ghosh
PhD candidate, IIT Jodhpur



Introduction

IDS: Intrusion Detection System

- Monitors network or system activity for malicious behavior or policy violations.
- Detects attacks such as port scanning, brute-force attempts, malware communication, etc.

IPS: Intrusion Prevention System

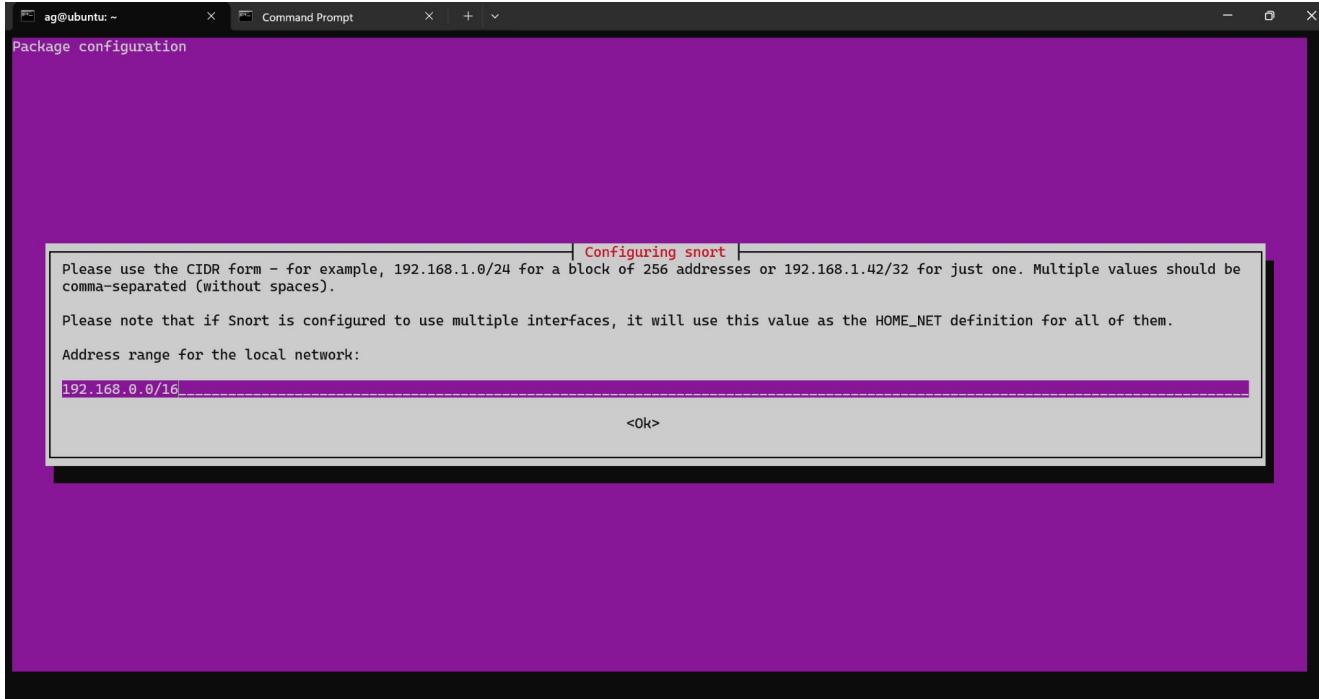
Snort

- An open-source network-based IDS/IPS.
- **IDS Mode** – Detects and alerts on suspicious traffic.
- **IPS Mode** – Detects and actively blocks suspicious traffic (with iptables + NFQUEUE integration).



Snort Installation

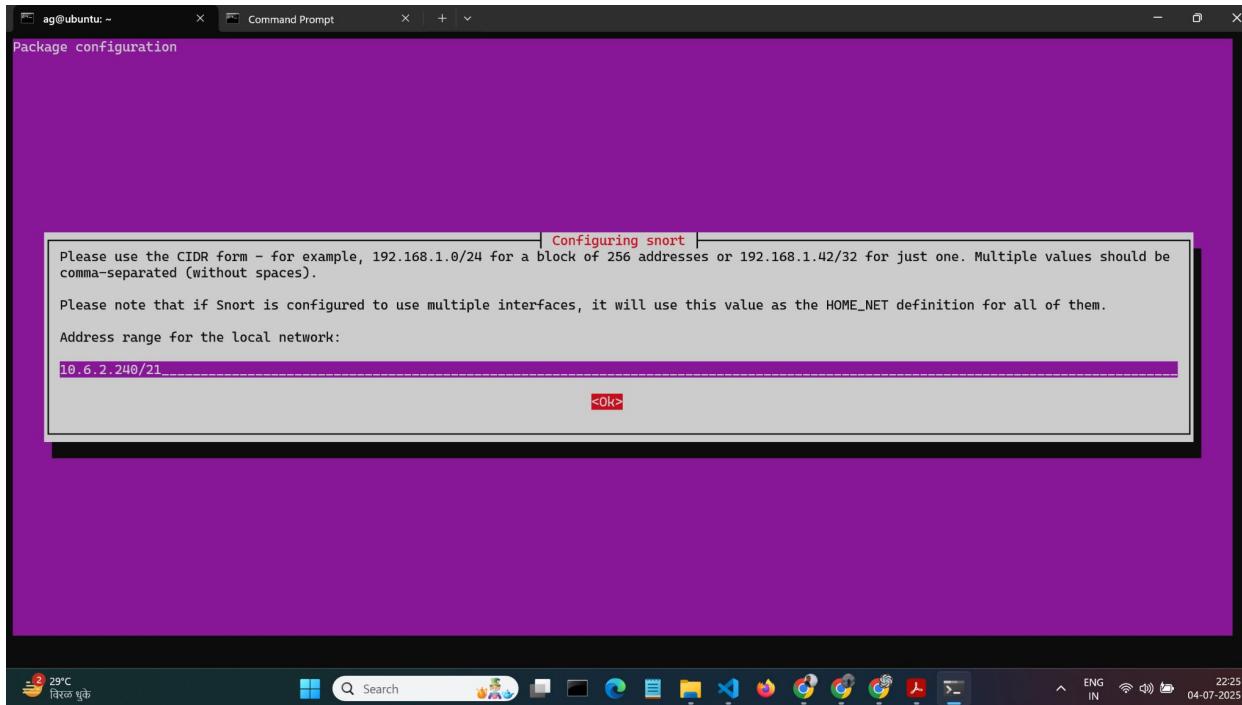
```
sudo apt install snort -y
```





Snort Installation

Setting up with IP (ip a) of device





Snort Installation

Verify installation: snort -V

```
ayana@Ayan:/etc/snort$ snort -V

      --> Snort! <--
Version 2.9.20 GRE (Build 82) x86_64
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

ayana@Ayan:/etc/snort$
```



Snort setup .conf file

sudo vim /etc/snort/snort.conf

```
ag@ubuntu: ~      x  Command Prompt      x  ayana@Ayan: ~      x  +  v
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
##### Step #1: Set the network variables. For more information, see README.variables #####
#####

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

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

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

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network

45,1          3%
```



Snort setup .conf file

Change to the HOME_NET IP

```
ag@ubuntu: ~      Command Prompt      ayana@Ayan: ~      - + 
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#####
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 10.6.2.248/21

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

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

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

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

62,1      4%
```



Snort setup .conf file

Comment out all 'include \$RULE_PATH...' if not done
Keep the 'include \$RULE_PATH/local.rules'

```
ag@ubuntu:/etc/snort      x  Command Prompt      x  ayana@Ayan: ~      x  +  x
#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/local.rules

# include $RULE_PATH/app-detect.rules
# include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/blacklist.rules
include $RULE_PATH/botnet-cnc.rules
include $RULE_PATH/browser-chrome.rules
include $RULE_PATH/browser-firefox.rules
include $RULE_PATH/browser-ie.rules
include $RULE_PATH/browser-other.rules
include $RULE_PATH/browser-plugins.rules
include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/file-executable.rules
include $RULE_PATH/file-flash.rules
include $RULE_PATH/file-identify.rules
include $RULE_PATH/file-image.rules
include $RULE_PATH/file-multimedia.rules
include $RULE_PATH/file-office.rules
include $RULE_PATH/file-other.rules
-- INSERT --
```



Snort setup .conf file

Change the 'var RULE_PATH' to '/etc/snort/rules' if not done

```
ag@ubuntu:/etc/snort      X  Command Prompt      X  ayana@Ayan: ~      X  +  v
# List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80

# List of ports you might see oracle attacks on
portvar ORACLE_PORTS 1024:

# List of ports you want to look for SSH connections on:
portvar SSH_PORTS 22

# List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]

# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5060]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.179.0/24,205.188.205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH ../../rules
var SO_RULE_PATH ../../so_rules
var PREPROC_RULE_PATH ../../preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
```

104,1

11%



Snort setup .conf file

Comment out the \$WHITE_LIST... and \$BLACK_LIST... paths block

```
ag@ubuntu: /etc/snort      x  Command Prompt      x  ayana@Ayan: ~      x  +  v
gp_decode_depth 0 \
bitenc_decode_depth 0 \
uu_decode_depth 0

# POP preprocessor. For more information see README.pop
preprocessor pop: \
ports { 110 } \
b64_decode_depth 0 \
gp_decode_depth 0 \
bitenc_decode_depth 0 \
uu_decode_depth 0

# Modbus preprocessor. For more information see README.modbus
preprocessor modbus: ports { 502 }

# DNP3 preprocessor. For more information see README.dnp3
preprocessor dnp3: ports { 20000 } \
memcap 262144 \
check_crc

# Reputation preprocessor. For more information see README.reputation
# preprocessor reputation: \
# memcap 500, \
# priority whitelist, \
# nested_ip inner, \
whitelist $WHITE_LIST_PATH/white_list.rules, \
blacklist $BLACK_LIST_PATH/black_list.rules

#####
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
#####

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

-- INSERT --
```

509,2

74%



Verify .conf file

sudo snort -T -c /etc/snort/snort.conf

```
ag@ubuntu:/etc/snort  x  Command Prompt  x  ayana@Ayan: ~  x  +  v  x  -  o  x
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
  Ports:
    502
DNP3 config:
  Memcap: 262144
  Check Link-Layer CRCs: ENABLED
  Ports:
    20000
Reputation config:
ERROR: /etc/snort/snort.conf(512) => Unable to open address file /etc/snort/../rules/white_list.rules, Error: No such file or directory
Fatal Error, Quitting..
ag@ubuntu:/etc/snort$ sudo vim snort.conf
ag@ubuntu:/etc/snort$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

      === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7
777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 4108
0 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 714
4:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 344
43:34444 41084 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
```



IDS : Custom ICMP rule

```
sudo vim /etc/snort/rules/local.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001;  
rev:1;)
```

```
ag@ubuntu: /etc/snort      X  Command Prompt      X  ayana@Ayan: /etc/snort      X  Command Prompt      X +   
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
# -----  
# LOCAL RULES  
# -----  
# This file intentionally does not come with signatures. Put your local  
# additions here.  
  
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)  
~  
~
```



IDS : Ping

sudo snort -A console -q -c /etc/snort/snort.conf -i <interface>
In my case: <interface> = eth0 (obtained from 'ip a')

```
ag@ubuntu:/etc/snort      x  Command Prompt      x  ayana@Ayan: ~      x  +  v
==== Initialization Complete ====
--> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_S7COMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>

Total snort Fixed Memory Cost - MaxRss:46720
Snort successfully validated the configuration!
Snort exiting
ag@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
07/04-23:48:38.242093 [**] [1:1000001:1] ICMP Packet Detected [**] [Priority: 0] {ICMP} 10.22.8.28 -> 10.6.2.240
07/04-23:48:48.228064 [**] [1:1000001:1] ICMP Packet Detected [**] [Priority: 0] {ICMP} 10.22.8.28 -> 10.6.2.240
07/04-23:48:49.239557 [**] [1:1000001:1] ICMP Packet Detected [**] [Priority: 0] {ICMP} 10.22.8.28 -> 10.6.2.240
07/04-23:48:50.249315 [**] [1:1000001:1] ICMP Packet Detected [**] [Priority: 0] {ICMP} 10.22.8.28 -> 10.6.2.240
07/04-23:48:51.258943 [**] [1:1000001:1] ICMP Packet Detected [**] [Priority: 0] {ICMP} 10.22.8.28 -> 10.6.2.240
```



IDS : Ping

Log file

```
sudo snort -A fast -q -c /etc/snort/snort.conf -i eth0
```

```
sudo cat /var/log/snort/alert
```

```
ayana@Ayan:/etc/snort$ sudo vim ./rules/local.rules
ayana@Ayan:/etc/snort$ sudo snort -A fast -q -c /etc/snort/snort.conf -i eth0
^Z
[2]+  Stopped                  sudo snort -A fast -q -c /etc/snort/snort.conf -i eth0
ayana@Ayan:/etc/snort$ sudo cat /var/log/snort/alert
07/04-19:14:51.353792  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:14:56.176277  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:15:01.183762  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:15:06.186023  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
ayana@Ayan:/etc/snort$
```



IPS : rule

```
drop icmp any any -> $HOME_NET any (msg:"ICMP Ping Dropped"; sid:1000002; rev:1;)
```

```
ag@ubuntu:/etc/snort      X  Command Prompt      X  ayana@Ayan:/etc/snort      X  Command Prompt      X  +  v
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

drop icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000002; rev:1;)
~
```



IPS : Traffic through Snort

```
sudo apt install libnetfilter-queue-dev -y (dependency)  
sudo snort -Q --daq nfq -c /etc/snort/snort.conf
```

```
sudo iptables -I INPUT -j NFQUEUE  
sudo iptables -I FORWARD -j NFQUEUE
```

This sends all incoming and forwarded traffic through Snort.



IPS : Ping blocked

Pings are blocked

```
C:\Users\ayana>ping 172.30.62.123 -n 4

Pinging 172.30.62.123 with 32 bytes of data:
Reply from 172.30.62.123: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.62.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ayana>ping 172.30.62.123 -n 4

Pinging 172.30.62.123 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.30.62.123:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Thank you

