

Ex. No: 7***Date:12/09/2025******SNORT IDS******AIM:***

To demonstrate Intrusion Detection System (IDS) using snort tool.

ALGORITHM:

1. Update the system using the package manager.
2. Install Snort 3 along with required libraries such as libpcap.
3. Verify the Snort 3 installation using the version command.
4. Create the necessary directories for rules and logs.
5. Create a custom rule file (local.rules) and add an ICMP alert rule.
6. Edit the Snort 3 configuration file (snort.lua) to load the custom rule file.
7. Identify the active network interface using the ip a command.
8. Start Snort 3 in IDS mode using the configuration file and the selected interface.
9. Generate ICMP traffic by pinging an external site from another terminal.
10. Open the Snort log directory and view the alert entries created for the ICMP packets.

COMMANDS :

sudo apt update

sudo apt install snort3 libpcap-dev -y

snort3 -V

sudo mkdir -p /etc/snort/rules

sudo mkdir -p /var/log/snort

sudo nano /etc/snort/rules/local.rules

(Inside local.rules)

***alert icmp any any -> any any (msg:"ICMP Ping Detected - Snort3";
sid:1000001; rev:1;)***

sudo nano /etc/snort/snort.lua

ip a

sudo snort3-c /etc/snort/snort.lua-ieth0

(Open another terminal)

ping yahoo.com

OUTPUT:

```
(JackSparrow@Captain)-[~]
$ snort --version

'''-
o" )~
'''

--> Snort++ <*-
Version 3.1.82.0
By Martin Roesch & The Snort Team
http://snort.org/contact#team
Copyright (C) 2014-2024 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using DAQ version 3.0.12
Using LuaJIT version 2.1.1700206165
Using OpenSSL 3.5.2 5 Aug 2025
Using libpcap version 1.10.5 (with TPACKET_V3)
Using PCRE version 8.39 2016-06-14
Using ZLIB version 1.3.1
Using LZMA version 5.8.1
```

```
(JackSparrow@Captain)-[~]
$ ping yahoo.com
PING yahoo.com (74.6.231.20) 56(84) bytes of data.
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=1 ttl=52 time=348 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=2 ttl=52 time=371 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=3 ttl=52 time=292 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=4 ttl=52 time=314 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=5 ttl=52 time=337 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=6 ttl=52 time=360 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=7 ttl=52 time=282 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=8 ttl=52 time=302 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=9 ttl=52 time=325 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=10 ttl=52 time=348 ms
64 bytes from media-router-fp73.prod.media.vip.net.yahoo.com (74.6.231.20): icmp_seq=11 ttl=52 time=370 ms
```

```
(JackSparrow@Captain)-[~]
$ sudo snort -c /etc/snort/snort.lua -i eth0
[sudo] password for JackSparrow:
-----
o")~   Snort++ 3.1.82.0
-----

Loading /etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
```

```
pcap DAQ configured to passive.  
Commencing packet processing  
++ [0] eth0  
^C** caught int signal  
== stopping  
-- [0] eth0
```

Packet Statistics

daq

```
received: 119  
analyzed: 119  
allow: 119  
rx_bytes: 11102
```

codec

```
total: 119      (100.000%)  
arp: 10         ( 8.403%)  
eth: 119        (100.000%)  
icmp4: 109      ( 91.597%)  
ipv4: 109       ( 91.597%)
```

Module Statistics

appid

```
packets: 109  
processed_packets: 109  
total_sessions: 1
```

arp_spoof

```
packets: 10
```

binder

```
raw_packets: 10  
new_flows: 1  
inspects: 11
```

detection

```
analyzed: 119
```

port_scan

```
packets: 109  
trackers: 2
```

stream

```
flows: 1
```

stream_icmp

```
sessions: 1  
max: 1  
created: 1  
released: 1
```

Summary Statistics

process

```
signals: 1
```

timing

```
runtime: 00:01:17  
seconds: 77.271477  
pkts/sec: 2
```

```
o")~ Snort exiting
```

RESULT:

Thus, the Intrusion Detection System (IDS) has been successfully demonstrated using snort.