

# Assignment 6: SNORT Configuration

Karthikeyan G

Roll Number: CB.SC.P2CYS24008

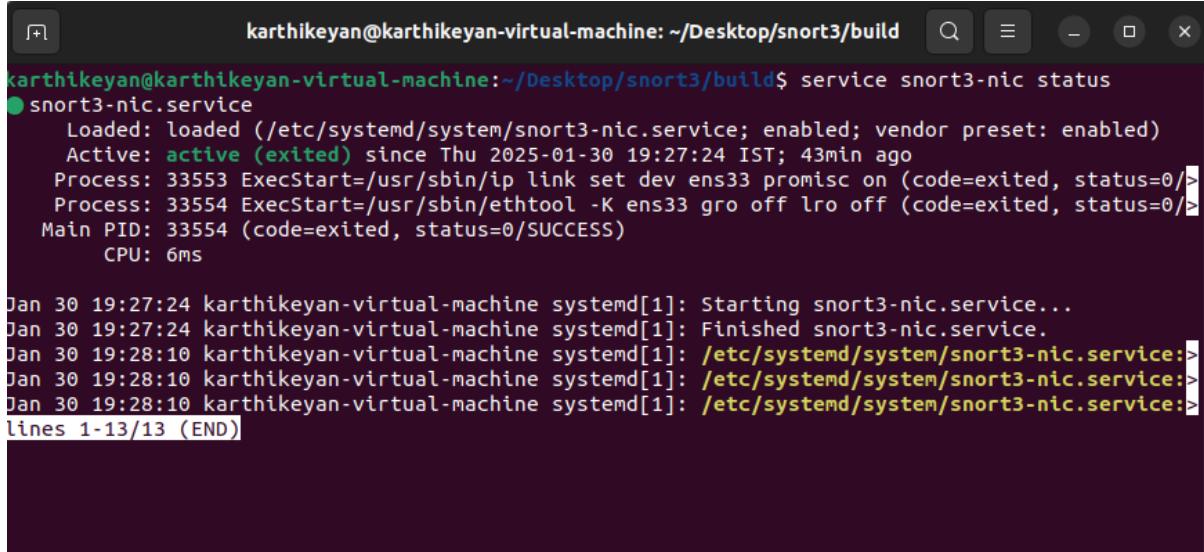
January 30, 2025

## 1. Installation and Configuration

```
karthikeyan@karthikeyan-virtual-machine:~/Documents$ snort -V
,,_
o" )~ -*> Snort++ <*-
'``' Version 3.6.2.0
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 3.0.18
Using libpcap version 1.10.1 (with TPACKET_V3)
Using LuaJIT version 2.1.0-beta3
Using LZMA version 5.2.5
Using OpenSSL 3.0.2 15 Mar 2022
Using PCRE2 version 10.39 2021-10-29
Using ZLIB version 1.2.11
```

Figure 1: Installation and configuration of SNORT. This step involves downloading and setting up SNORT on the system, ensuring all dependencies are met and the software is correctly installed.

## Install SNORT and Ensure It Is Running

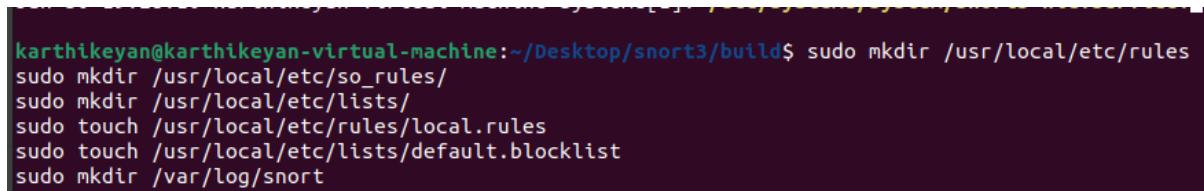


```
kartikeyan@kartikeyan-virtual-machine:~/Desktop/snort3/build$ service snort3-nic status
● snort3-nic.service
  Loaded: loaded (/etc/systemd/system/snort3-nic.service; enabled; vendor preset: enabled)
  Active: active (exited) since Thu 2025-01-30 19:27:24 IST; 43min ago
    Process: 33553 ExecStart=/usr/sbin/ip link set dev ens33 promisc on (code=exited, status=0)
    Process: 33554 ExecStart=/usr/sbin/ethtool -K ens33 gro off lro off (code=exited, status=0)
  Main PID: 33554 (code=exited, status=0/SUCCESS)
    CPU: 6ms

Jan 30 19:27:24 kartikeyan-virtual-machine systemd[1]: Starting snort3-nic.service...
Jan 30 19:27:24 kartikeyan-virtual-machine systemd[1]: Finished snort3-nic.service.
Jan 30 19:28:10 kartikeyan-virtual-machine systemd[1]: /etc/systemd/system/snort3-nic.service:>
Jan 30 19:28:10 kartikeyan-virtual-machine systemd[1]: /etc/systemd/system/snort3-nic.service:>
Jan 30 19:28:10 kartikeyan-virtual-machine systemd[1]: /etc/systemd/system/snort3-nic.service:>
lines 1-13/13 (END)
```

Figure 2: SNORT is successfully installed and running. This verification step ensures that SNORT is operational and ready for further configuration.

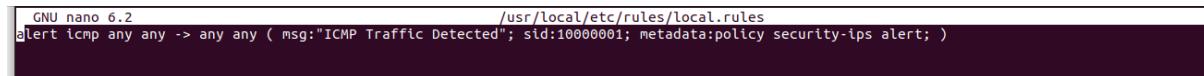
## Create Folders and Files Required by SNORT for Rules



```
kartikeyan@kartikeyan-virtual-machine:~/Desktop/snort3/build$ sudo mkdir /usr/local/etc/rules
sudo mkdir /usr/local/etc/so_rules/
sudo mkdir /usr/local/etc/lists/
sudo touch /usr/local/etc/rules/local.rules
sudo touch /usr/local/etc/lists/default.blocklist
sudo mkdir /var/log/snort
```

Figure 3: Necessary folders and files for SNORT rules are created. This includes directories for storing custom rules and configuration files essential for SNORT's operation.

## Add a Rule to Detect ICMP Traffic in the local.rules File



```
GNU nano 6.2                                     /usr/local/etc/rules/local.rules
alert icmp any any -> any any ( msg:"ICMP Traffic Detected"; sid:10000001; metadata:policy security-ips alert; )
```

Figure 4: A custom rule is added to the local.rules file to detect ICMP traffic. This rule helps in identifying and logging ICMP packets, which are commonly used in network diagnostics and attacks.

## Start SNORT and Load the local.rules File Using the -R Parameter

```
karthikeyan@karthikeyan-virtual-machine:~/Desktop/snort3/build$ sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules
-----
o")~ Snort++ 3.6.2.0
-----
Loading /usr/local/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
    ssh
    host_cache
    pop
    so_proxy
    stream_tcp
    mms
    smtp
    gtp_inspect
    packets
```

Figure 5: SNORT is started with the local.rules file loaded using the -R parameter. This ensures that the custom rules are active and SNORT is monitoring traffic according to the specified rules.

## Run SNORT in Detection Mode on an Interface and Log All Alarms

```
pcap DAQ configured to passive.
Commencing packet processing
++ [0] ens33
```

Figure 6: SNORT is running in detection mode on a specified network interface, logging all alarms. This mode allows SNORT to monitor traffic and generate alerts based on the configured rules.

## Generate ICMP Traffic and Verify That the Alert Is Not Triggered

The image shows two terminal windows side-by-side. The left terminal window, titled 'Terminal' and running on 'karthikeyan@karthikeyan-virtual-machine', displays the output of the command 'snort -c /usr/local/etc/snort/snort.lua'. The output shows various configuration details such as rule counts, service rule counts, fast pattern groups, search engine instances, and memory usage. It also indicates that PCAP DAQ is configured to passive and that packet processing has commenced. The right terminal window, titled 'Activities Terminal' and running on 'seed@VM: ~', shows a continuous stream of ICMP traffic being captured. The logs show numerous ICMP packets from source IP 192.168.133.133, with sequence numbers ranging from 970 to 999. Each packet is 64 bytes long, has a TTL of 64, and a time of 0.00 ms to 1.99 ms.

```

ties Terminal Jan 30 21:20
karthikeyan@karthikeyan-virtual-machine: ~/Desktop... karthikeyan@karthikeyan-virtual-machine: ~/Desktop...
root@karthikeyan-virtual-machine: ~ root@karthikeyan-virtual-machine: ~
karthikeyan@karthikeyan-virtual-machine: ~ karthikeyan@karthikeyan-virtual-machine: ~
/usr/local/etc/snort/snort.lua

rule counts
total rules loaded: 219
text rules: 219
option chains: 219
chain headers: 1

service rule counts
to-srv to-clt
file id: 219 219
total: 219 219

fast pattern groups
to-server: 1
to-client: 1

search engine (ac_bnf)
instances: 2
patterns: 438
pattern memory: 1832
num states: 1832
memory scale: KB
total memory: 71.2812
pattern memory: 19.6484
match memory: 28.4375
transition memory: 22.9453
appid: MaxBss diff: 3200
appid: pattern loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] ens33

Activities Terminal Jan 30 10:50
Activities Terminal Jan 30 10:50
seed@VM: ~ seed@VM: ~
64 bytes from 192.168.133.133: icmp_seq=970 ttl=64 time=1.19 ms
64 bytes from 192.168.133.133: icmp_seq=971 ttl=64 time=1.99 ms
64 bytes from 192.168.133.133: icmp_seq=972 ttl=64 time=1.08 ms
64 bytes from 192.168.133.133: icmp_seq=973 ttl=64 time=1.02 ms
64 bytes from 192.168.133.133: icmp_seq=974 ttl=64 time=1.31 ms
64 bytes from 192.168.133.133: icmp_seq=975 ttl=64 time=3.09 ms
64 bytes from 192.168.133.133: icmp_seq=976 ttl=64 time=1.06 ms
64 bytes from 192.168.133.133: icmp_seq=977 ttl=64 time=1.13 ms
64 bytes from 192.168.133.133: icmp_seq=978 ttl=64 time=0.477 ms
64 bytes from 192.168.133.133: icmp_seq=979 ttl=64 time=0.827 ms
64 bytes from 192.168.133.133: icmp_seq=980 ttl=64 time=0.849 ms
64 bytes from 192.168.133.133: icmp_seq=981 ttl=64 time=1.04 ms
64 bytes from 192.168.133.133: icmp_seq=982 ttl=64 time=0.558 ms
64 bytes from 192.168.133.133: icmp_seq=983 ttl=64 time=2.31 ms
64 bytes from 192.168.133.133: icmp_seq=984 ttl=64 time=1.01 ms
64 bytes from 192.168.133.133: icmp_seq=985 ttl=64 time=1.36 ms
64 bytes from 192.168.133.133: icmp_seq=986 ttl=64 time=0.729 ms
64 bytes from 192.168.133.133: icmp_seq=987 ttl=64 time=1.27 ms
64 bytes from 192.168.133.133: icmp_seq=988 ttl=64 time=0.992 ms
64 bytes from 192.168.133.133: icmp_seq=989 ttl=64 time=0.663 ms
64 bytes from 192.168.133.133: icmp_seq=990 ttl=64 time=1.56 ms
64 bytes from 192.168.133.133: icmp_seq=991 ttl=64 time=1.19 ms
64 bytes from 192.168.133.133: icmp_seq=992 ttl=64 time=0.612 ms
64 bytes from 192.168.133.133: icmp_seq=993 ttl=64 time=0.412 ms
64 bytes from 192.168.133.133: icmp_seq=994 ttl=64 time=0.882 ms
64 bytes from 192.168.133.133: icmp_seq=995 ttl=64 time=2.13 ms
64 bytes from 192.168.133.133: icmp_seq=996 ttl=64 time=0.639 ms
64 bytes from 192.168.133.133: icmp_seq=997 ttl=64 time=0.739 ms
64 bytes from 192.168.133.133: icmp_seq=998 ttl=64 time=0.782 ms
64 bytes from 192.168.133.133: icmp_seq=999 ttl=64 time=0.608 ms

```

Figure 7: Attempts to generate ICMP traffic and verify that the alert is not triggered. Despite following various configurations and referring to the guide at this link, no output was observed even after 30 minutes. Network settings were also adjusted, but no results were obtained.