

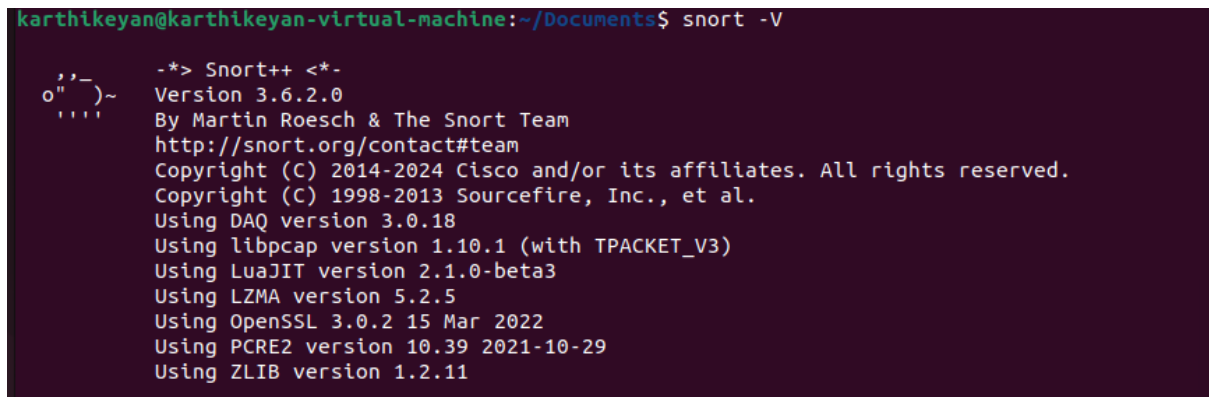
Assignment 6: SNORT Configuration

Karthikeyan G

Roll Number: CB.SC.P2CYS24008

January 30, 2025

1. Installation and Configuration

A terminal window with a dark purple background. The prompt is 'karthikeyan@karthikeyan-virtual-machine:~/Documents\$'. The command 'snort -V' has been executed, resulting in a multi-line output. The output starts with a decorative ASCII art logo on the left, followed by the text: '-*> 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', and 'Using ZLIB version 1.2.11'.

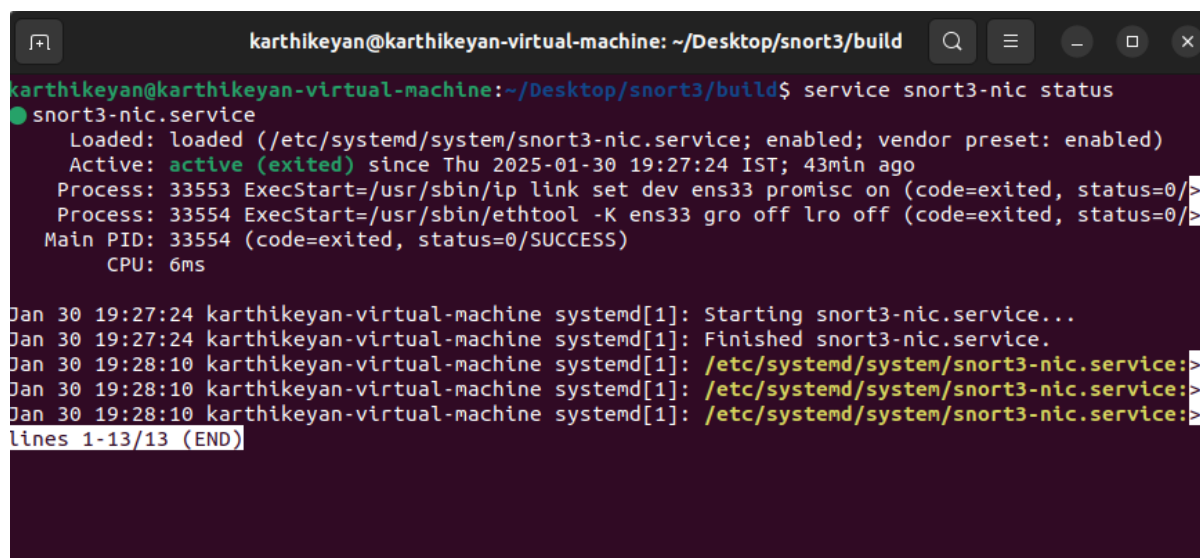
```
karthikeyan@karthikeyan-virtual-machine:~/Documents$ snort -V

,,-
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

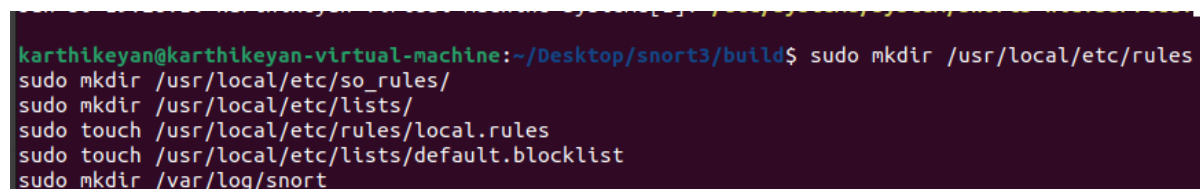


```
karthikeyan@karthikeyan-virtual-machine: ~/Desktop/snort3/build
karthikeyan@karthikeyan-virtual-machine:~/Desktop/snort3/build$ service snort3-nic status
● snort3-nic.service
   Loaded: loaded (/etc/systemd/system/snort3-nic.service; enabled; vendor preset: enabled)
   Active: active (exited) since 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 karthikeyan-virtual-machine systemd[1]: Starting snort3-nic.service...
Jan 30 19:27:24 karthikeyan-virtual-machine systemd[1]: Finished snort3-nic.service.
Jan 30 19:28:10 karthikeyan-virtual-machine systemd[1]: /etc/systemd/system/snort3-nic.service: >
Jan 30 19:28:10 karthikeyan-virtual-machine systemd[1]: /etc/systemd/system/snort3-nic.service: >
Jan 30 19:28:10 karthikeyan-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.

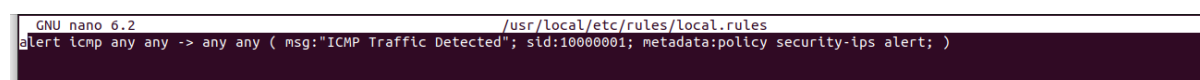
Create Folders and Files Required by SNORT for Rules



```
karthikeyan@karthikeyan-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.

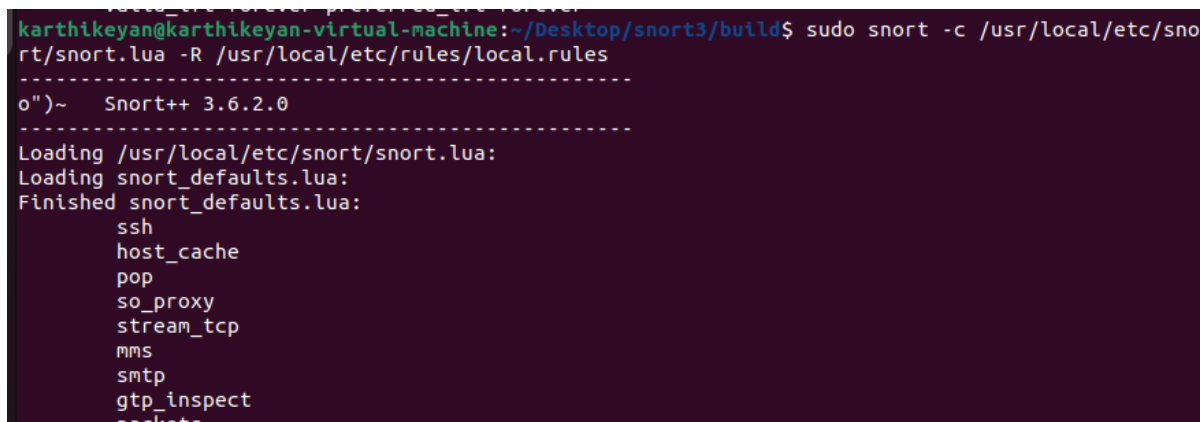
Add a Rule to Detect ICMP Traffic in the local.rules File



```
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.

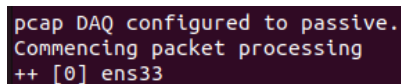
Start SNORT and Load the local.rules File Using the -R Parameter

A terminal window with a dark purple background. The prompt is 'karthikeyan@karthikeyan-virtual-machine:~/Desktop/snort3/build\$'. The command entered is 'sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules'. The output shows 'Snort++ 3.6.2.0' followed by a list of loaded modules: 'ssh', 'host_cache', 'pop', 'so_proxy', 'stream_tcp', 'mms', 'smtp', 'gtp_inspect', and 'packets'.

```
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

A terminal window with a dark purple background. The output shows 'pcap DAQ configured to passive.', 'Commencing packet processing', and '++ [0] ens33'.

```
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

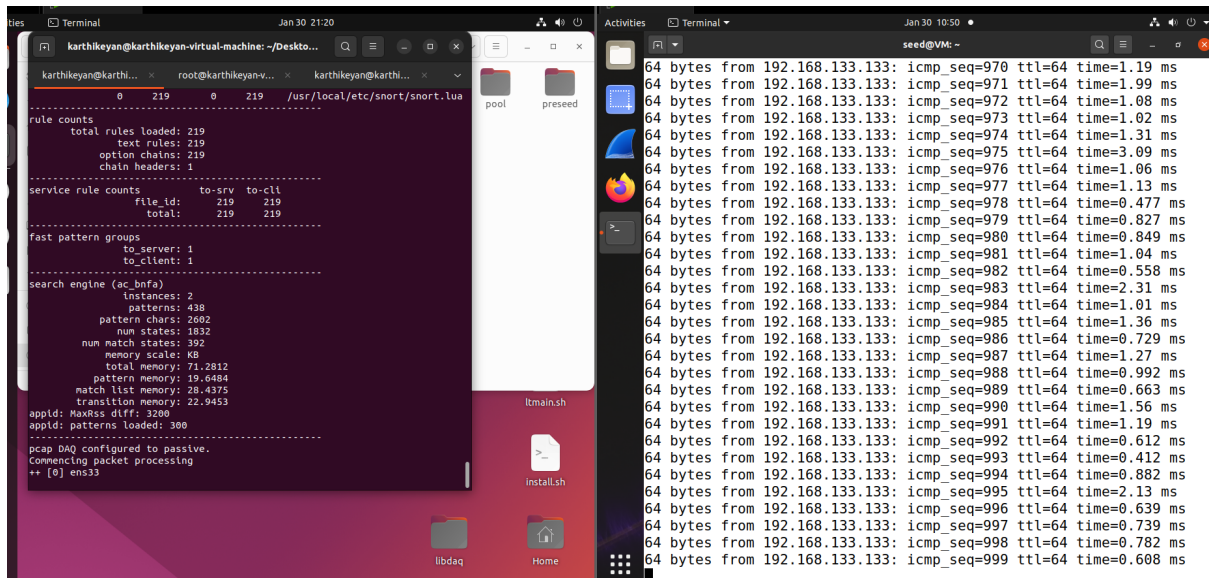


Figure 7: Attempts to generate ICMP traffic and verify that the alert is not triggered. Despite following various configurations and referring to the guide at this link, no output was observed even after 30 minutes. Network settings were also adjusted, but no results were obtained.