# 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

   ,,_     -*> Snort++ <*-
  o"  )~   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

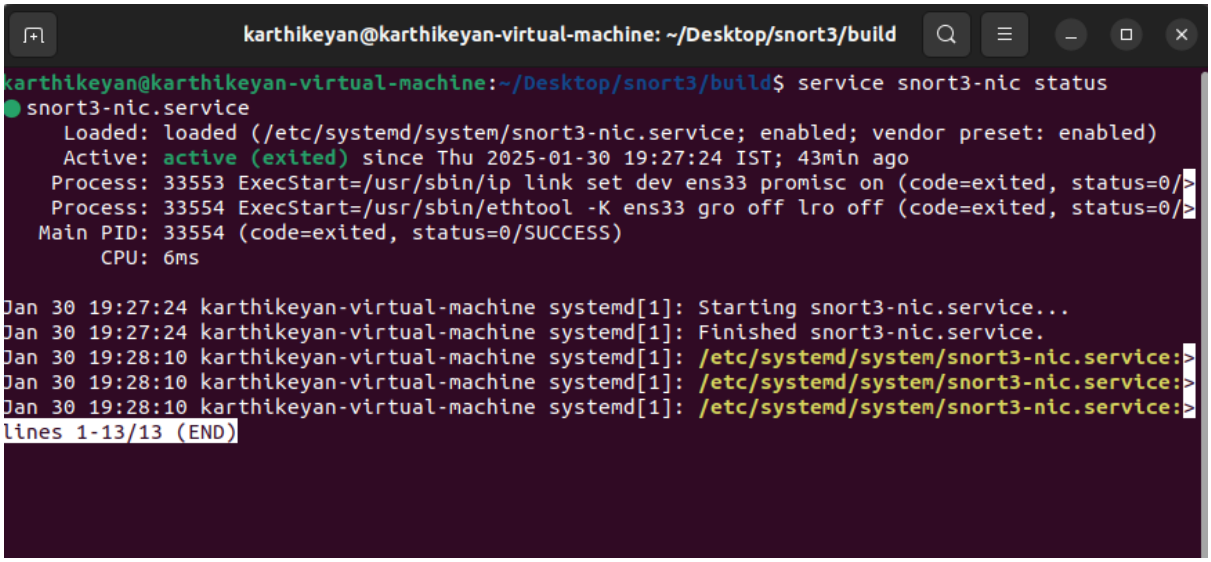


Figure 2: SNORT is successfully installed and running. This verification step ensures that SNORT is operational and ready for further configuration.

# Create Folders and Files Required by SNORT for Rules

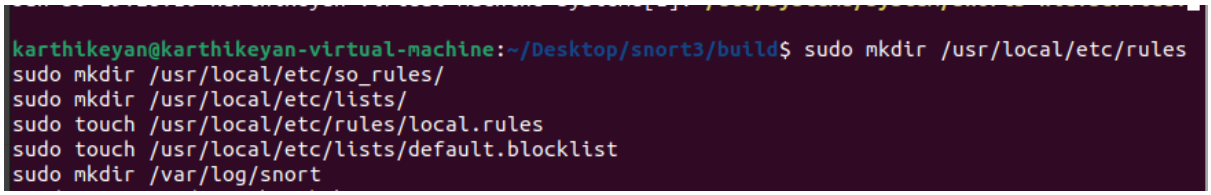


Figure 3: Necessary folders and files for SNORT rules are created. This includes directories for storing custom rules and configuration files essential for SNORT's operation.

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

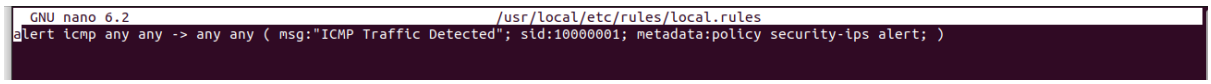


Figure 4: A custom rule is added to the local.rules file to detect ICMP traffic. This rule helps in identifying and logging ICMP packets, which are commonly used in network diagnostics and attacks.

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


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


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

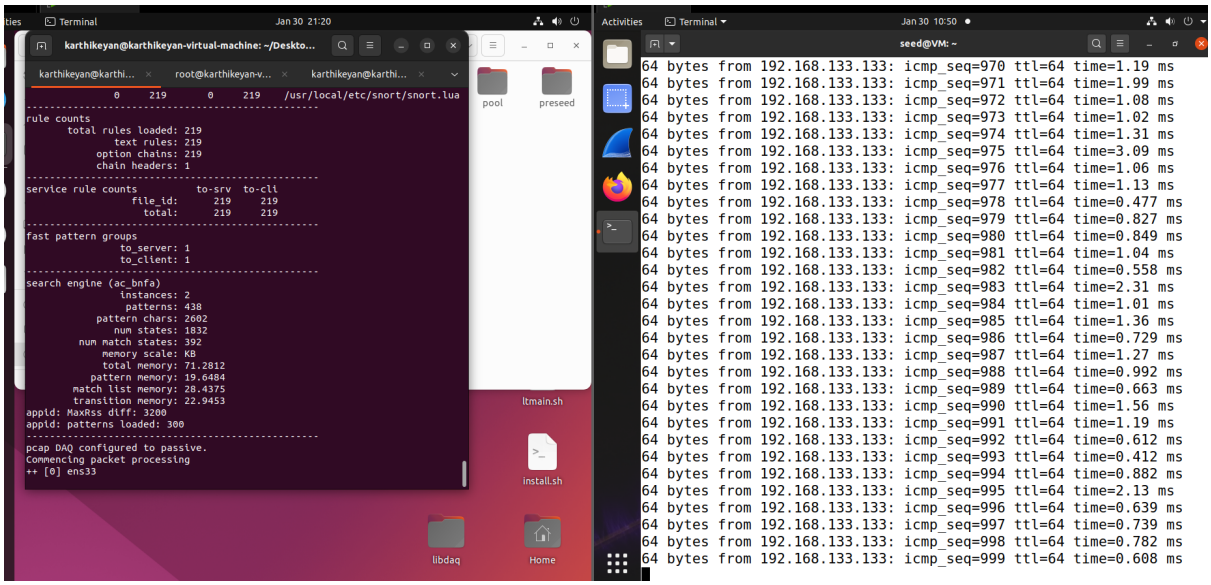


Figure 7: Attempts to generate ICMP traffic and verify that the alert is not triggered. Despite following various configurations and referring to the guide at this link, no output was observed even after 30 minutes. Network settings were also adjusted, but no results were obtained.