INSTITUTE FOR ADVANCED COMPUTING AND SOFTWARE DEVELOPMENT

AKURDI, PUNE

DOCUMENTATION ON

# “Automated Intrusion Monitoring with Snort Via Mail Alerts”

PG-DITISS March-2023

*SUBMITTED BY:*

**GROUP NO: 03**

**ASHWINI MHASKAR (233409)**

**SANIKA PAWASHE (233443)**

# MR. KARTIK AWARI MR. ROHIT PURANIK

## PROJECT GUIDE CENTRE CO-ORDINATOR

**TABLE OF CONTENTS**

TOPICS PAGE NO.

## ABSTRACT

## INTRODUCTION 1

## SNORT 2

## BARNYARD 3

* 1. MariaDB

## SMTP SERVER 5

* 1. DNS
  2. Email Alerts

## REQUIREMENT SPECIFICATION 8

* 1. Hardware requirements
  2. Software requirements
  3. Tools

## SCREENSHOTS 9

* 1. Snort
  2. Barnyard
  3. SMTP

## ADVANTAGES AND DISADVANTAGES 25

* 1. Advantages
  2. Disadvantages

## CONCLUSION 26

1. **REFERENCE 27**

# ABSTRACT

The "Automated Intrusion Monitoring with Snort via Mail Alerts" project presents an innovative solution to strengthen network security by leveraging the capabilities of the Snort intrusion detection system combined with automated email alerts. In today's dynamic and interconnected digital landscape, proactive intrusion detection is vital to safeguard sensitive data and critical systems. This project focuses on creating an automated framework that continually monitors network traffic, detects potential intrusion attempts using Snort's advanced rulesets, and promptly notifies administrators through email alerts. The project's central goal is to streamline the process of intrusion detection and response. By configuring Snort to analyze incoming network packets and employing customizable rulesets, the system can effectively identify suspicious patterns indicative of intrusion attempts. When such activities are detected, the system automatically generates detailed alerts, containing essential information about the nature of the attack and the compromised system.

Integration with an email alerting mechanism ensures that administrators remain informed in real-time. The project incorporates tools like Swatch or rsyslog to monitor Snort alerts in syslog messages and trigger immediate email notifications. This approach enables administrators to swiftly react to potential threats, enhancing incident response times and minimizing the impact of security breaches. Automation plays a crucial role, as scheduled scans and event-driven actions minimize manual intervention and enhance system efficiency. The project's holistic approach addresses various aspects of intrusion monitoring, from rule customization to automated alert generation, ensuring a comprehensive and adaptable solution.

# INTRODUCTION

In the realm of modern cyber security, the ability to detect and respond to potential network intrusions in real-time is paramount. The project "Automated Intrusion Monitoring with Snort via Mail Alert" aims to address this critical need by harnessing the power of Snort, a widely-used open-source network intrusion detection and prevention system. The project's primary focus is on automating the intrusion monitoring process and facilitating immediate alerts through email notifications. The project "Automated Intrusion Monitoring with Snort via Mail Alert" focuses on enhancing network security through automated intrusion detection and real-time alerts. By creating custom detection rules and integrating email alerts, the project enhances proactive threat management, ensuring that security teams can take immediate actions to mitigate risks. This project is designed to fortify network defenses and minimize the impact of security incidents.

The first objective is to implement a robust and sophisticated intrusion detection system using Snort. This system will continuously monitor network traffic for any signs of suspicious or malicious activities. The second objective involves the creation of custom detection rules tailored to the organization's unique network environment and threat landscape. These rules will be carefully crafted to detect specific intrusion attempts, such as port scans, brute-force attacks, and other unauthorized activities. The third objective centers around the integration of an automated email alerting mechanism. When the Snort system detects potential security breaches based on the custom rules, an automated script will trigger immediate email notifications to designated security personnel.

# SNORT

Snort is an open-source network intrusion detection and prevention system (NIDS/NIPS) developed by Sourcefire, which is now a part of Cisco. It is widely used in the field of cybersecurity to monitor network traffic for signs of malicious activities or unauthorized access attempts. Snort's primary function is to analyze network packets in real- time and compare them against a set of predefined rules to identify potential security threats.

Snort is used for several important reasons in the field of cybersecurity and network monitoring:

* **Intrusion Detection**: Snort is primarily used as an intrusion detection system (IDS) to identify unauthorized or malicious activities within a network. It analyzes network traffic and compares it against a set of predefined rules to detect known attack patterns and anomalies.
* **Packet Analysis**: Snort captures and analyzes network packets as they flow through a network interface, allowing it to inspect the content, headers, and metadata of these packets.
* **Real-Time Threat Detection: S**nort operates in real-time, allowing it to detect and alert on security threats as they happen. This rapid response capability is crucial for minimizing the potential damage caused by cyberattacks.
* Snort's rule-based detection approach allows organizations to tailor the system to their specific security needs. Custom rules can be created to identify unique threats that are relevant to a particular network environment.

**Rule-Based Detection:**

* **Preventive and Responsive**: Snort not only detects threats but can also be configured to take active responses, such as blocking or modifying traffic. This preventive action can mitigate the impact of attacks.
* **Real-Time Alerts:** When Snort identifies a packet that matches a predefined rule, it generates an alert. This alert can be logged in various formats, including text files, databases, and syslog, and can be used to notify administrators of potential security incidents.

# BARNYARD

Barnyard2 is a critical component often used alongside Snort, an open-source network intrusion detection and prevention system (NIDS/NIPS). Barnyard2 acts as a "post-processor" for Snort's generated alerts, enhancing the overall efficiency and management of intrusion detection efforts. It assists in processing and forwarding alerts to various output destinations, such as databases, log management systems, and security information and event management (SIEM) platforms.

Key Functions of Barnyard2:

* **Alert Processing:** When Snort identifies potential security threats in the network traffic, it generates alerts. Barnyard2 takes these alerts and processes them to create a more streamlined and manageable output.
* **Alert Unification:** Snort can produce alerts in various formats, such as binary and unified2. Barnyard2 unifies these diverse alert formats into a consistent and structured output.
* **Database Integration:** Barnyard2 can forward alerts to databases like MySQL, PostgreSQL, and SQLite. This integration facilitates easier querying and analysis of historical intrusion events.
* **Flexible Output:** It can output alerts to different destinations, including SIEM solutions, log management systems, and custom scripts, ensuring alerts reach the appropriate stakeholders.
* **Rule Management:** Barnyard2 can also manage Snort's rules, ensuring the ruleset is up-to-date and facilitating rule management tasks.

# MariaDB

MariaDB is an open-source relational database management system (RDBMS) that is a fork of MySQL. It was created as an alternative to MySQL after concerns arose about its acquisition by Oracle Corporation, which led to the development of an independent and community-driven database system. MariaDB aims to be a drop-in replacement for MySQL, offering compatibility while also introducing additional features and improvements.

Key aspects of MariaDB include:

* + - **Fork of MySQL:** MariaDB was initially created as a fork of MySQL, which means it shares a common ancestry with MySQL. As a result, many applications and tools that work with MySQL can also work with MariaDB without major modifications.
    - **Open Source:** Just like MySQL, MariaDB is an open-source database system released under the GNU General Public License (GPL). This allows anyone to use, modify, and distribute the software freely.
    - **Security Enhancements:** MariaDB includes security features like data-at-rest encryption, improved authentication methods, and the ability to segregate privileges based on roles.
    - **High Availability and Clustering:** MariaDB offers built-in features for replication, clustering, and high availability. This makes it suitable for applications requiring robust data redundancy and failover capabilities.

# SMTP SERVER

SMTP stands for Simple Mail Transfer Protocol. It is a standard protocol used for sending and receiving email messages over the Internet. SMTP servers play a crucial role in facilitating the transfer of email messages from the sender's email client to the recipient's email server. They are responsible for routing, relaying, and delivering email messages to their intended recipients.

Key features and functions of an SMTP server include:

* **Message Transfer**: SMTP servers are responsible for transferring email messages from the sender's email client (or originating email server) to the recipient's email server. This involves connecting to the recipient's email server and delivering the message.
* **Relaying:** SMTP servers can act as relays, forwarding messages between different email servers. This allows messages to be routed through multiple servers before reaching their final destination.
* **Authentication:** Many SMTP servers require authentication from the sender before allowing message submission. This helps prevent unauthorized use of the server for sending spam or malicious emails.
* If the recipient's email server is temporarily unavailable, the SMTP server can queue the message for later delivery, ensuring that emails are not lost.

**Message Queueing**:

* Message Headers: SMTP servers add essential headers to the email message, including sender and recipient information, subject, and timestamp.

# DNS :

DNS stands for Domain Name System. It is a fundamental system used on the Internet to translate

human-readable domain names into numerical IP addresses that computers and network devices use to identify each other and communicate. DNS serves as a crucial component for the functioning of the modern internet, providing a decentralized and hierarchical naming system.

Key aspects of the DNS include:

* + - Domain names are user-friendly, text-based addresses used to access websites and online resources. For example, "[www.example.com](http://www.example.com/)" is a domain name.

**Domain Names**:

* + - IP addresses are numerical addresses assigned to devices connected to a network. They uniquely identify devices and allow data to be sent to the correct destination.

**IP Addresses**:

* + - **DNS Resolution:** When a user enters a domain name into a web browser, the browser sends a request to a DNS resolver (usually provided by the Internet Service Provider) to translate the domain name into an IP address.
    - **Name Servers:** DNS servers, also known as name servers, are responsible for storing and distributing DNS records. They maintain databases that map domain names to IP addresses.
    - **DNS Records:** DNS records contain information about domain names and their associated IP addresses. Common types of DNS records include A records (mapping domain names to IPv4 addresses), AAAA records (mapping to IPv6 addresses), MX records (identifying mail servers), and more.
    - **Forward and Reverse Lookup:** DNS performs both forward lookup (translating domain names to IP addresses) and reverse lookup (finding domain names associated with IP addresses).

# Email Alerts :

Email alerts, also known as email notifications or email notifications, are messages sent via email to inform individuals or groups about specific events, updates, or conditions. These alerts play a crucial role in keeping people informed about important developments in various contexts, including security, monitoring, communication, and business operations.

Key characteristics of email alerts include:

* **Event Notification:** Email alerts are triggered by specific events or conditions. These events can range from security breaches, system errors, and changes in status to transaction confirmations, account updates, and more.
* **Recipient List:** Email alerts are sent to designated recipients or groups of individuals who need to be informed about the event. Recipients can include administrators, employees, customers, clients, and stakeholders.
* **Automation:** Email alerts are often automated, triggered by predefined conditions or events. This ensures that recipients receive timely notifications without manual intervention.
* **Importance:** Email alerts communicate critical and time-sensitive information. They help recipients take appropriate action or make informed decisions based on the information provided.
* **Recipient List:** Email alerts are sent to designated recipients or groups of individuals who need to be informed about the event. Recipients can include administrators, employees, customers, clients, and stakeholders.
* **Network Security:** Email alerts can be set up to notify administrators about potential security breaches, intrusion attempts, or suspicious activities detected by security systems like firewalls and intrusion detection systems (IDS).

# 5. REQUIREMENT SPECIFICATION

## 5.1 Hardware Requirement:

## RAM: 16 GB

## HDD: 512 GB

## Software Requirement:

* Operating System: Debian
* Database : MariaDB

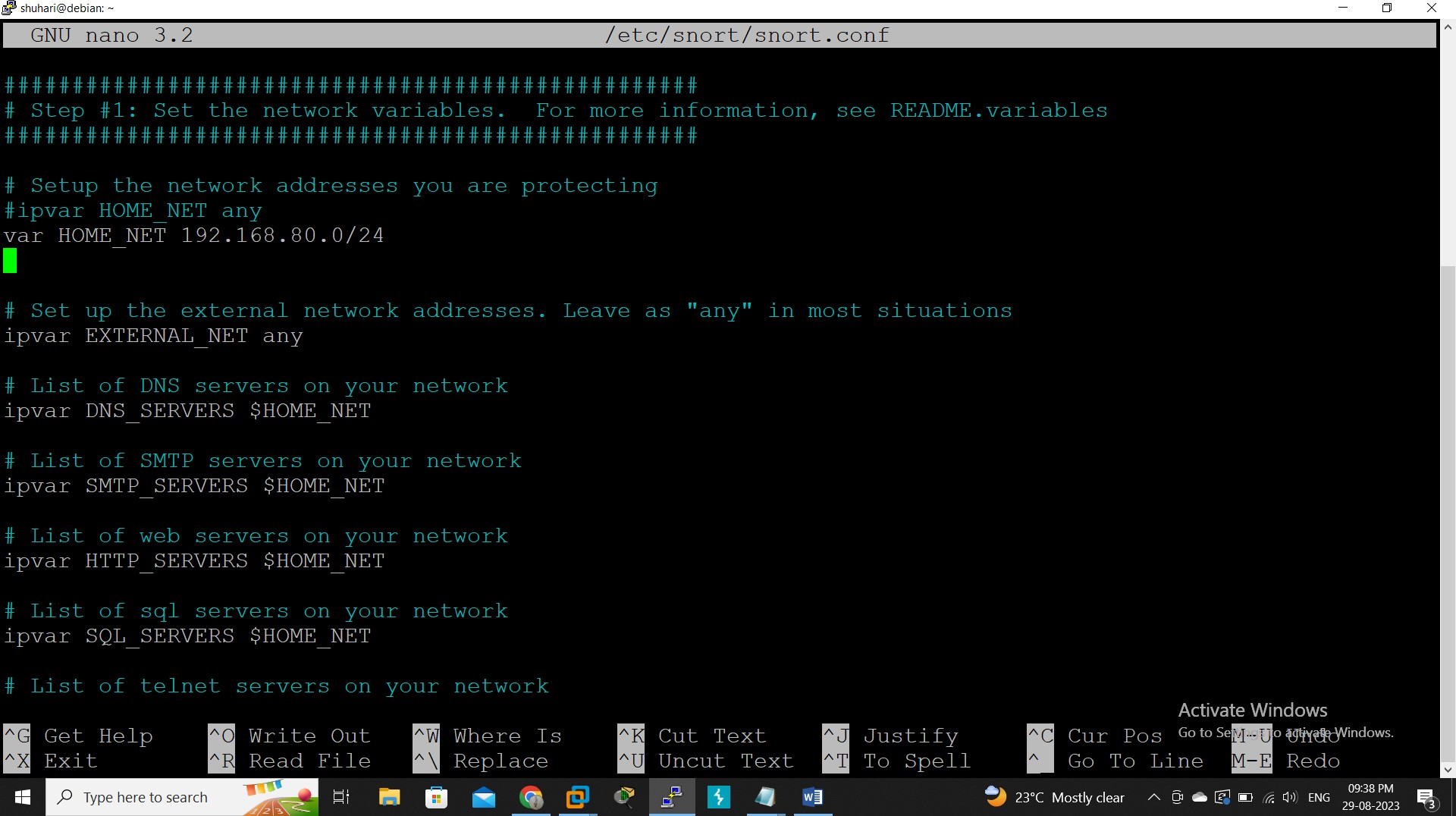
**5.3 Tools:**

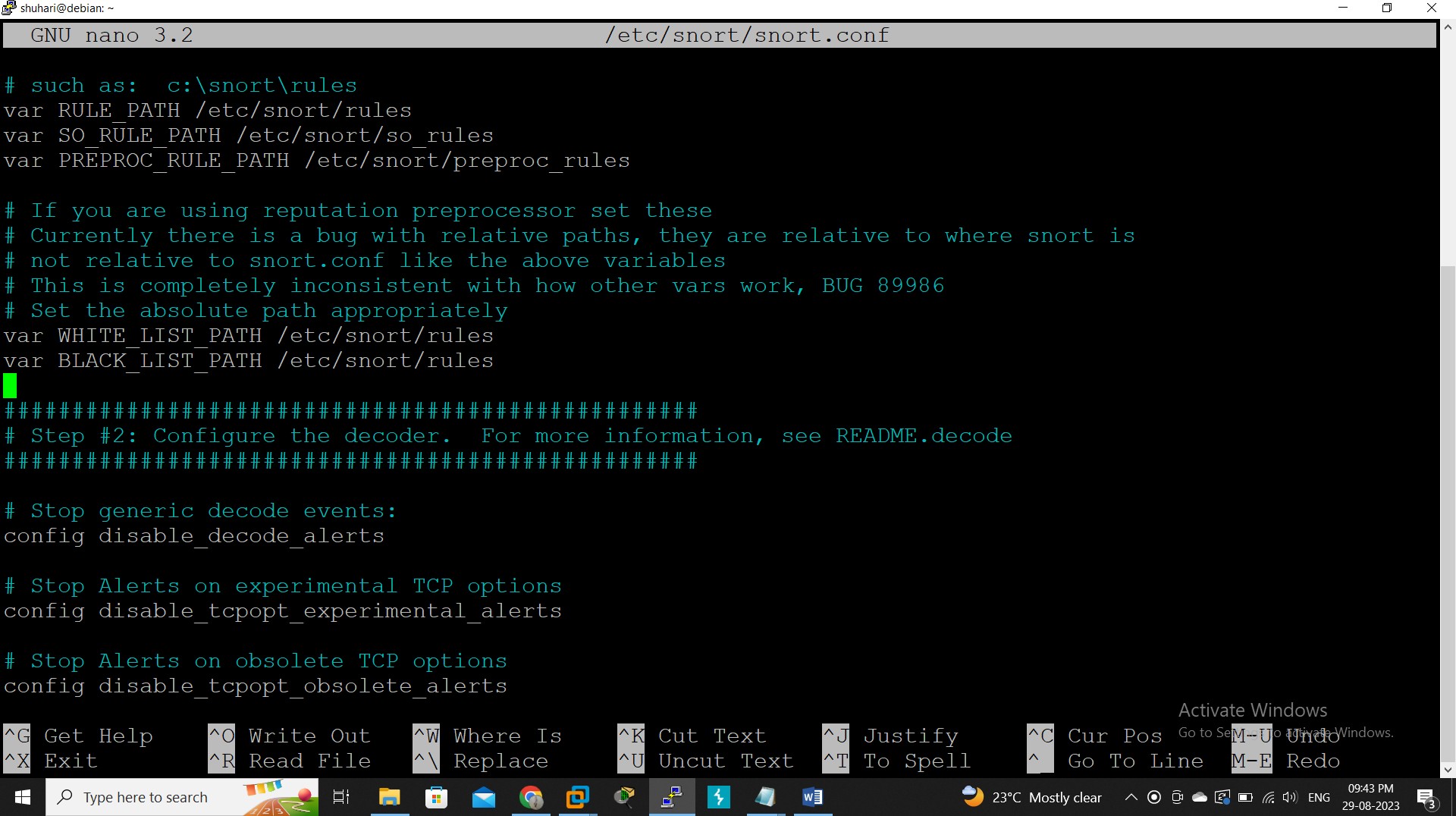
* Snort

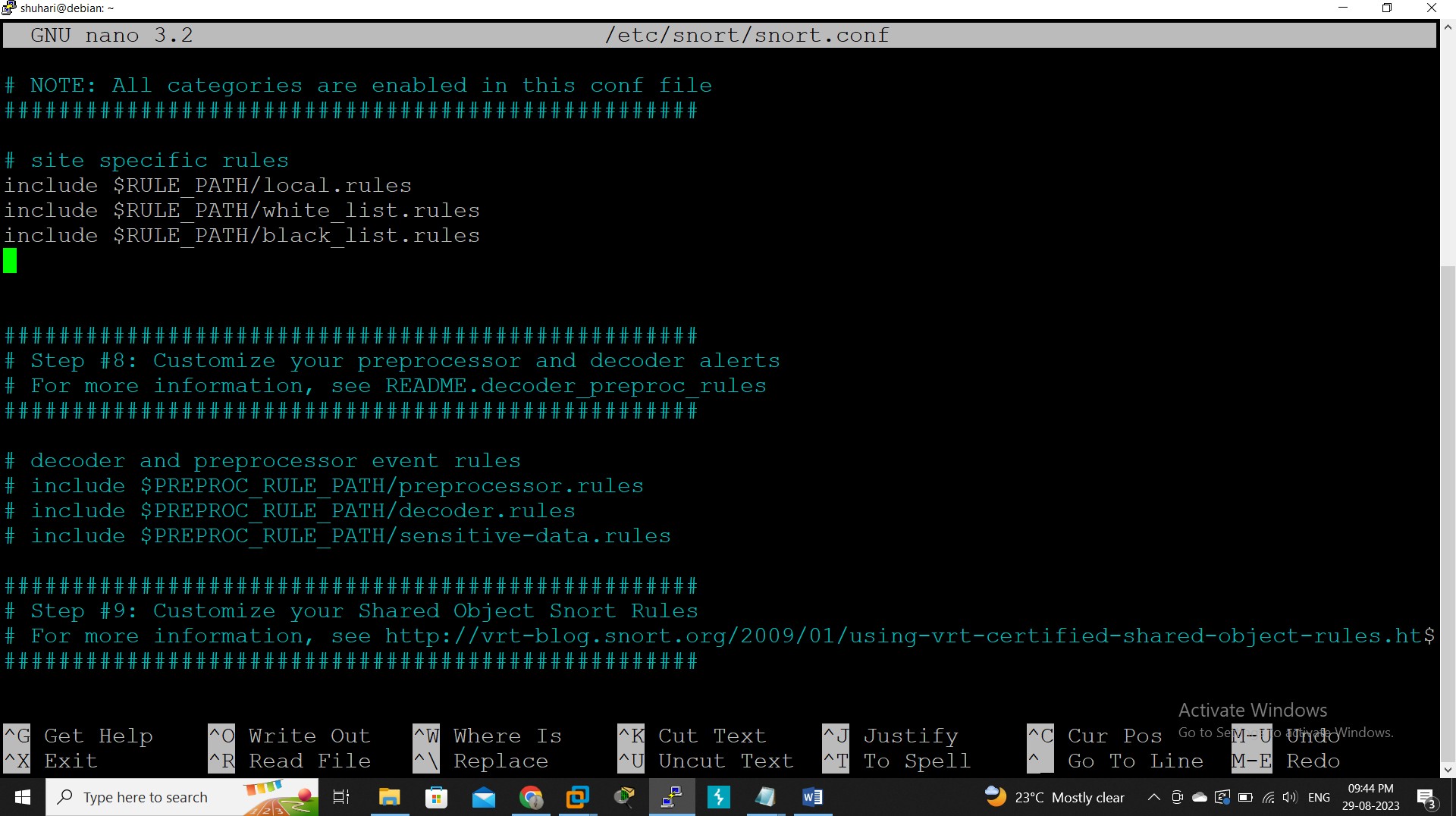
**6. SCREENSHOTS**

* 1. **Snort**

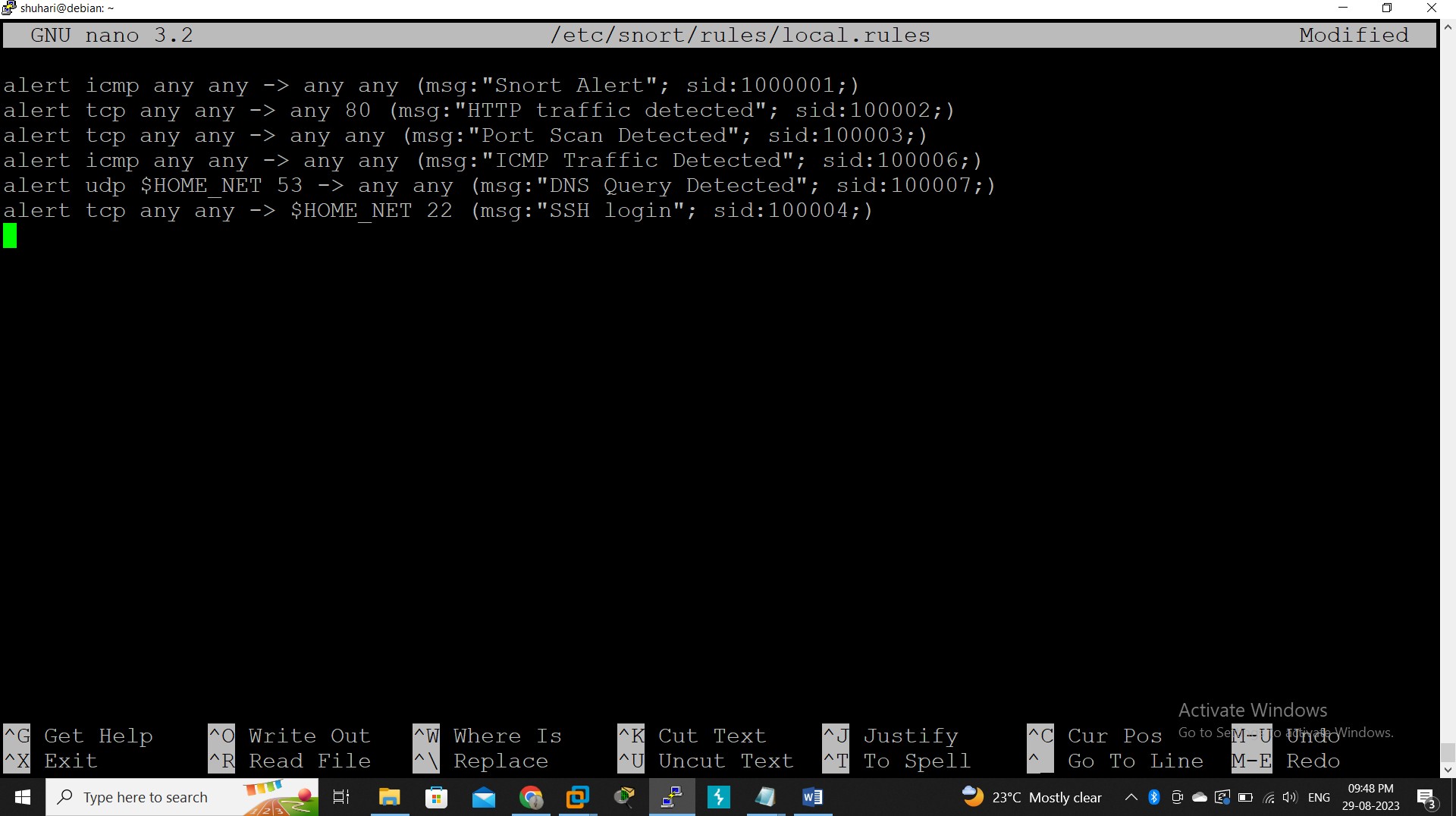
# Snort.conf





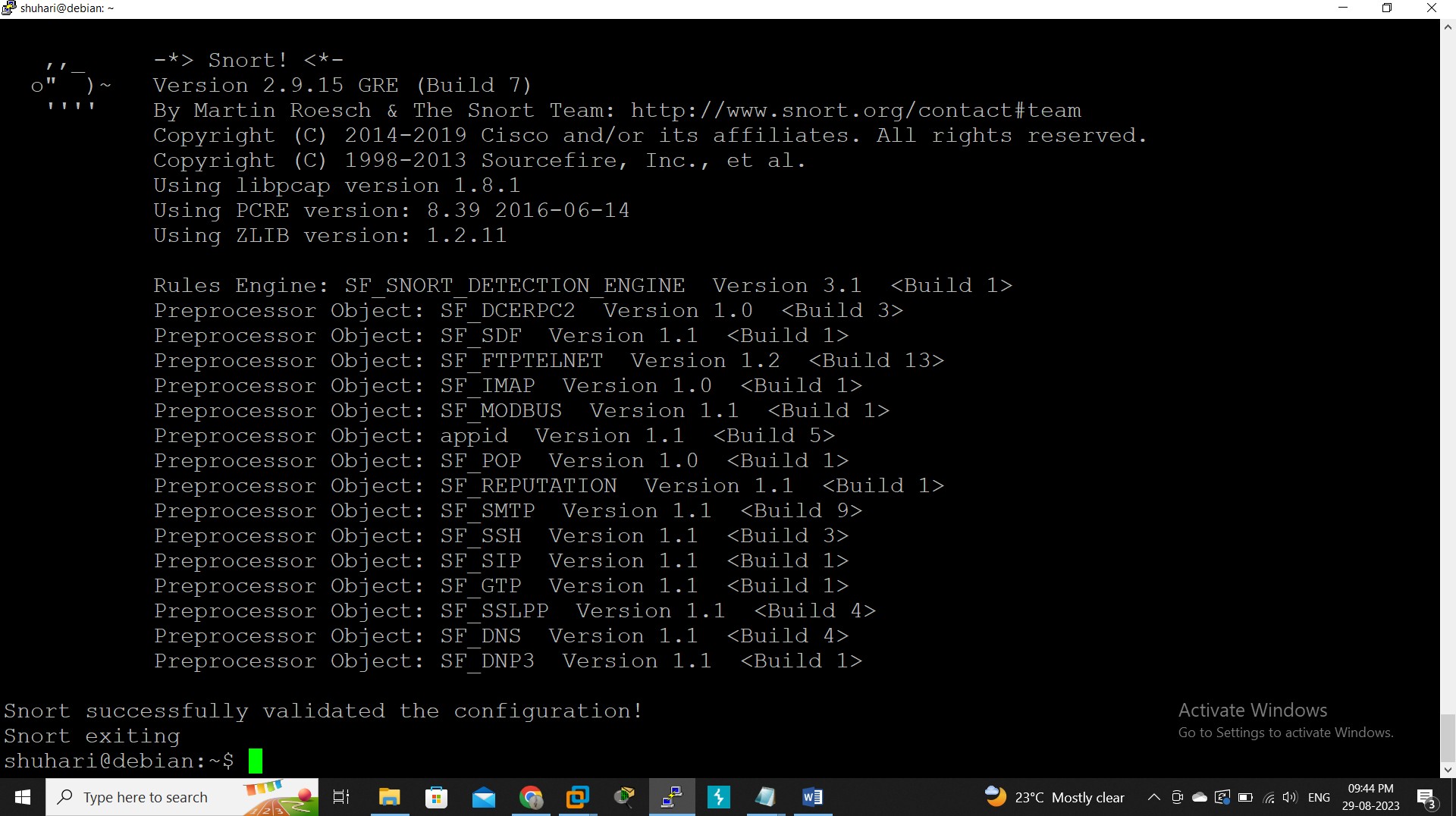


* + 1. **local.rules**

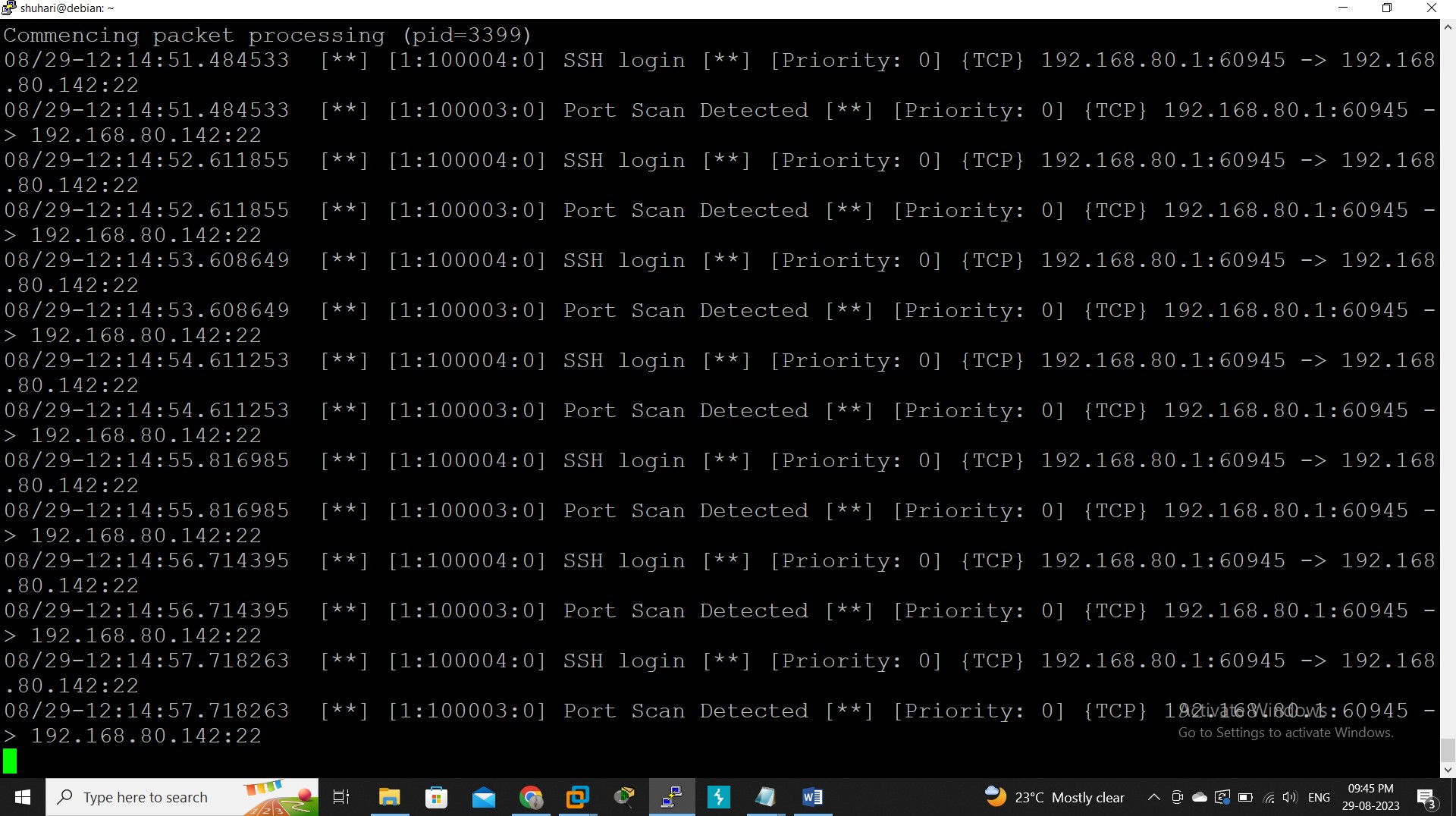


# Test Configuration

## Sudo snort –T –c /etc/snort/snort.conf

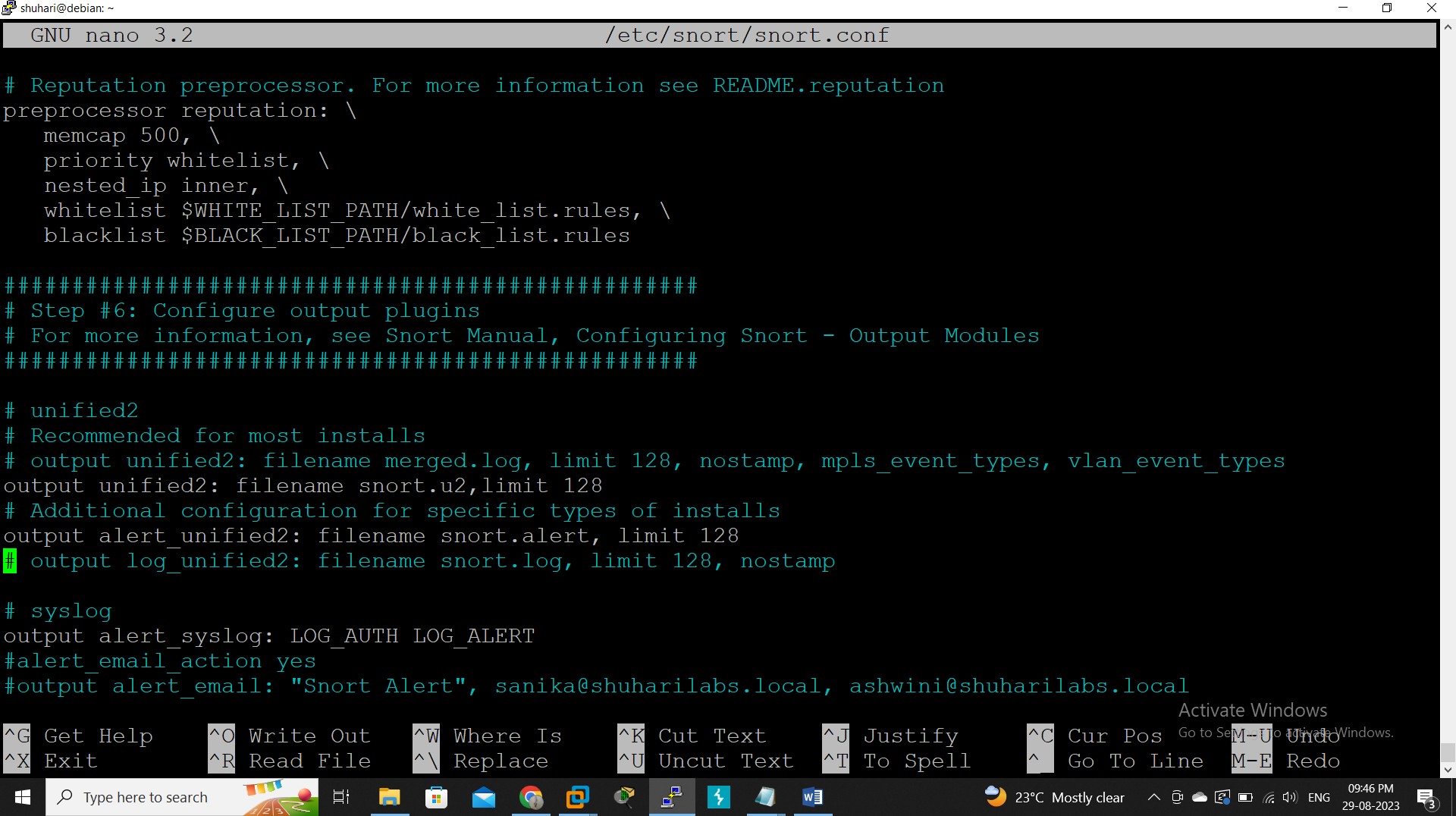


**Sudo snort –i ens33 –u snort –g snort –c /etc/snort/snort.conf –A console**



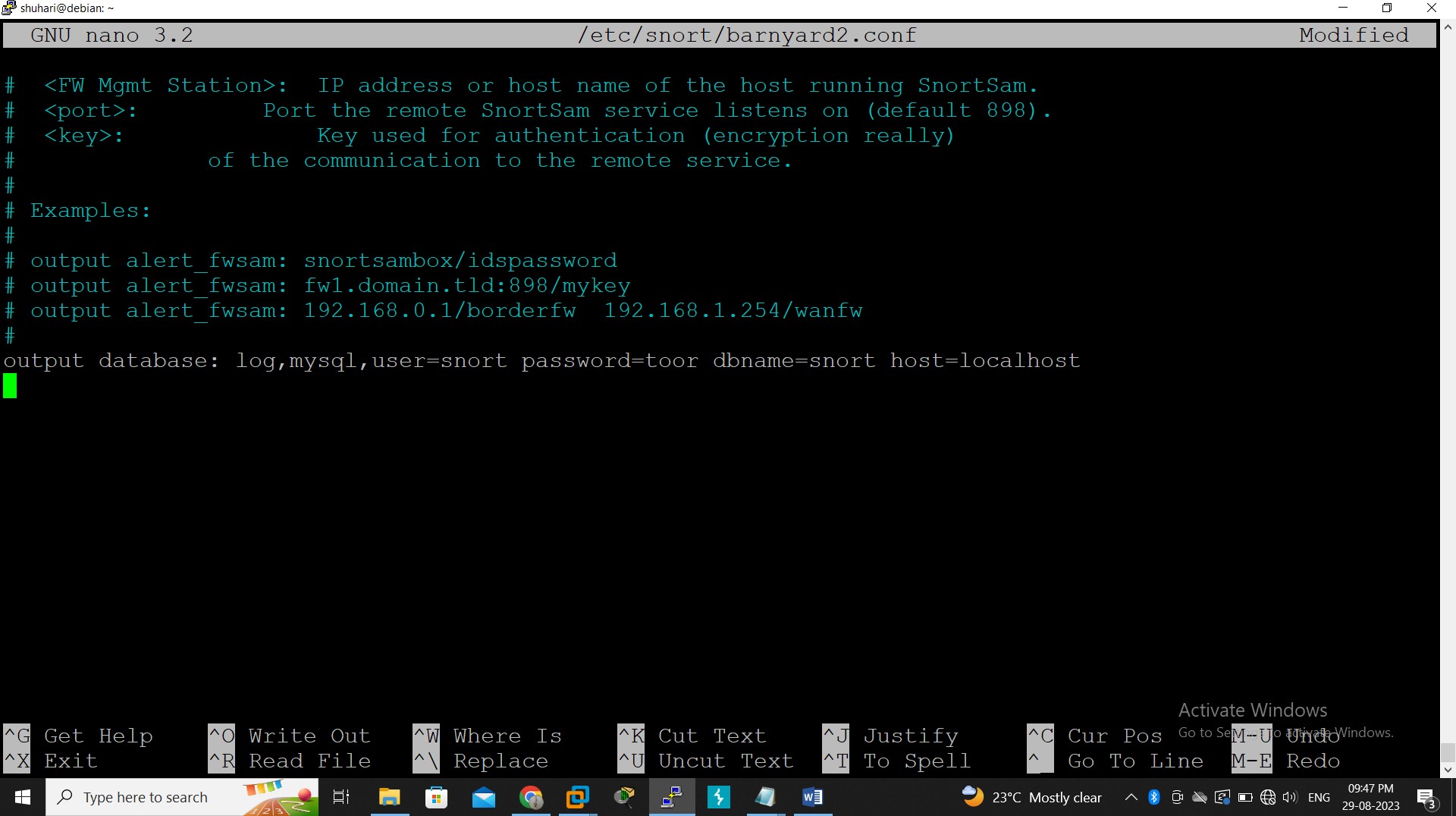
# Barnyard

**6.2.1 snort.conf**

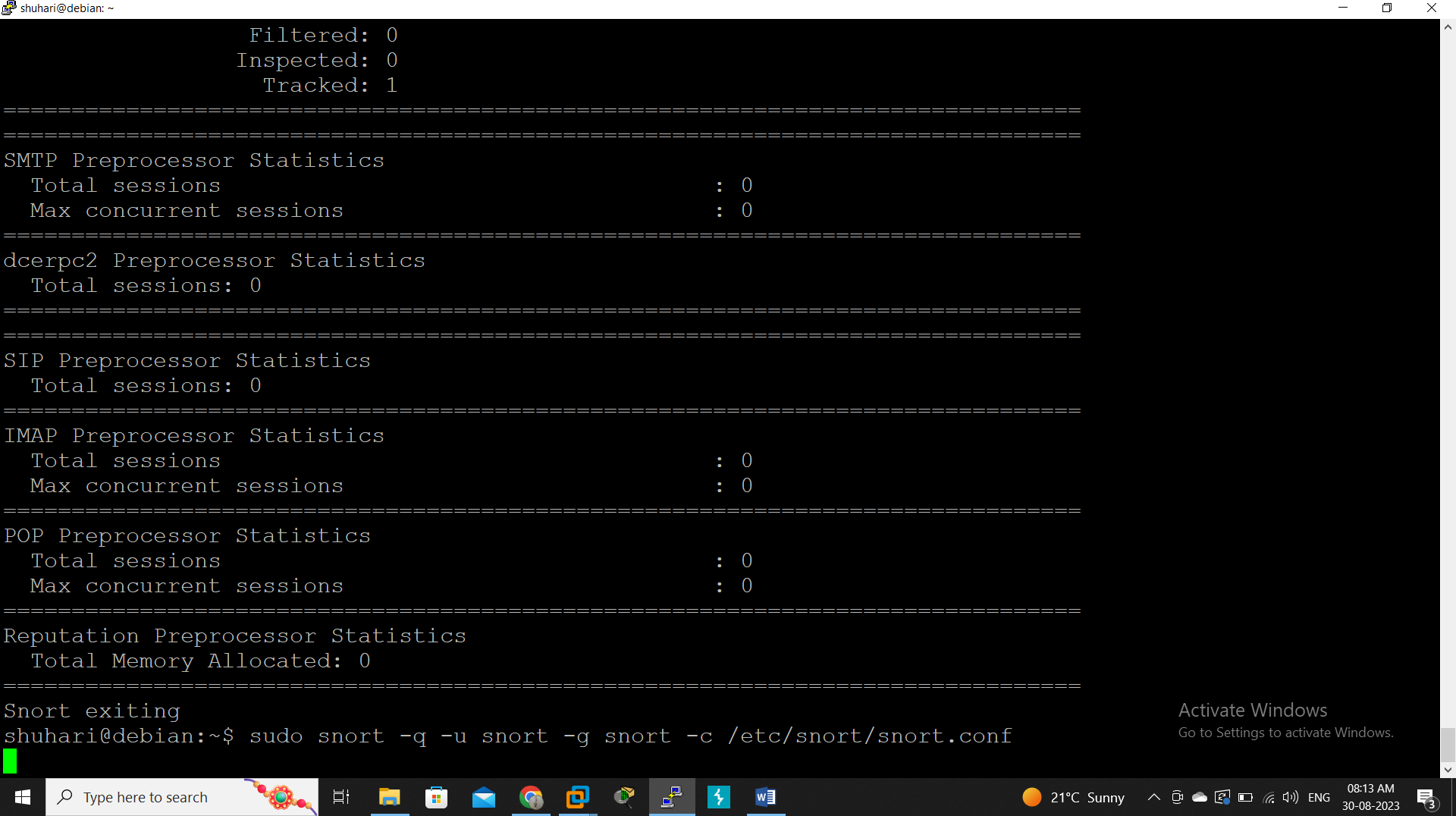


# 

# 6.2.2 barnyard.conf

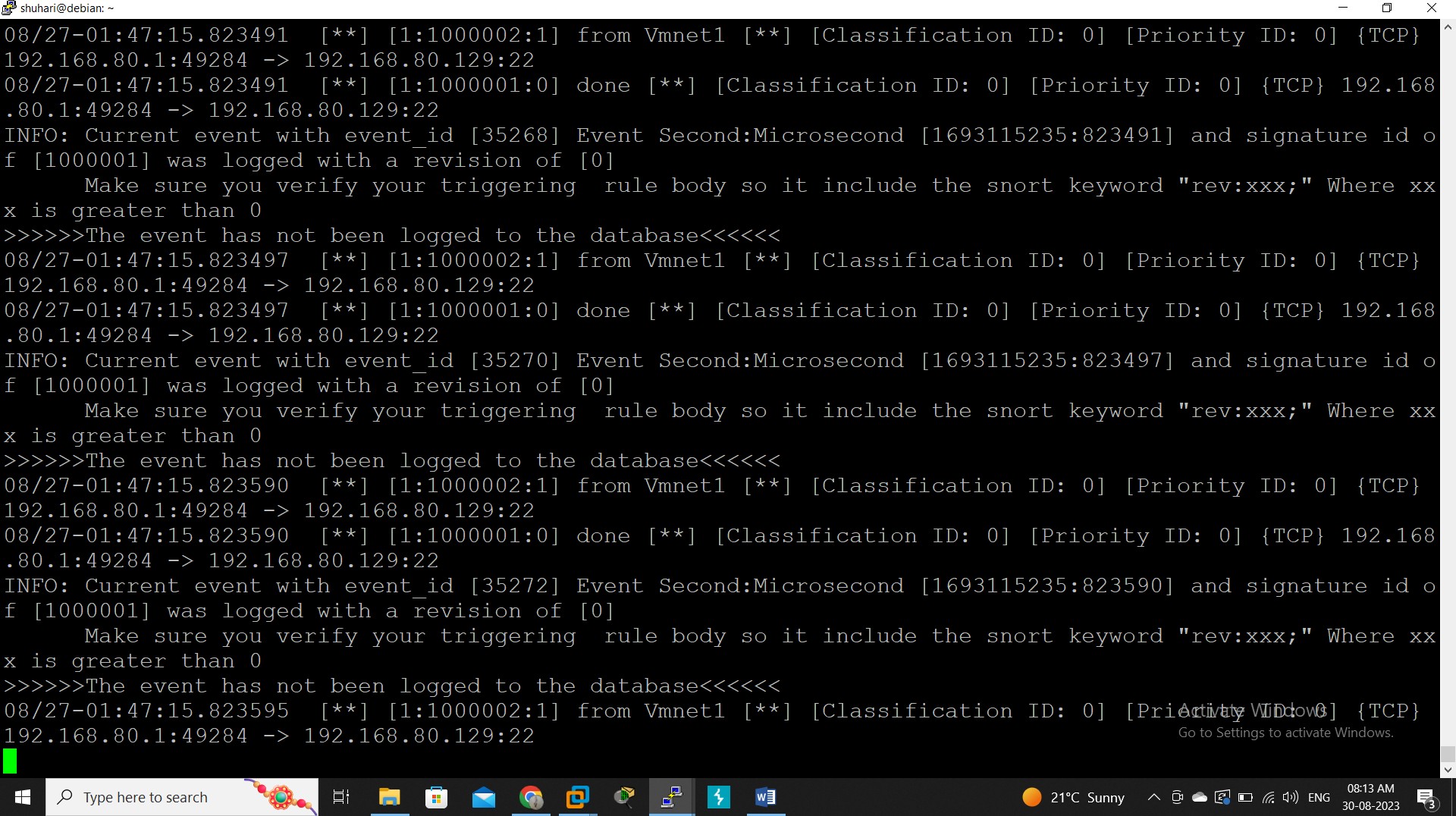


* + 1. **Test Configuration**

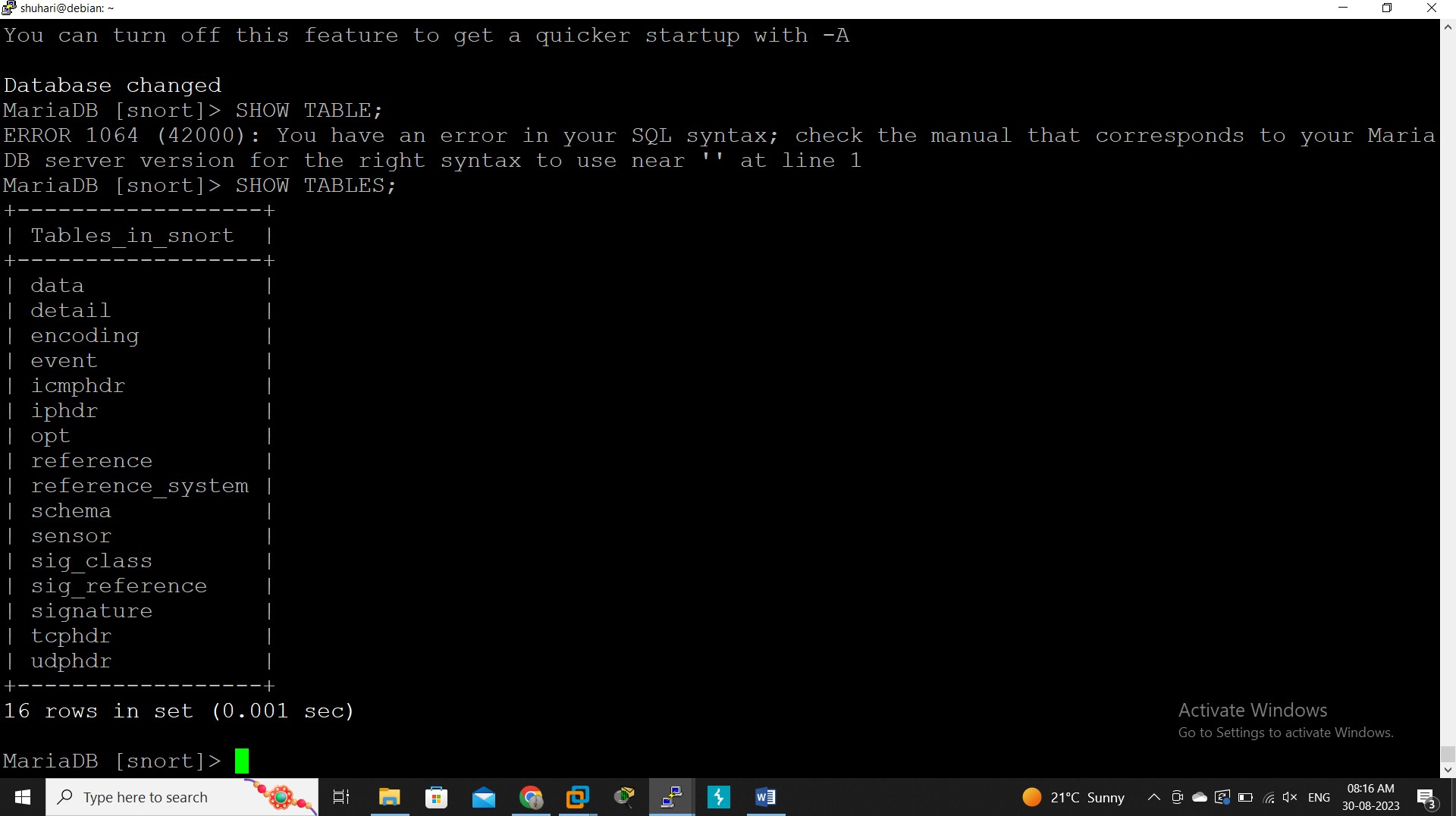


## Sudo barnyard2 –c /etc/snort/barnyard2.conf –d /var/log/snort/ -f snort.u2 –w

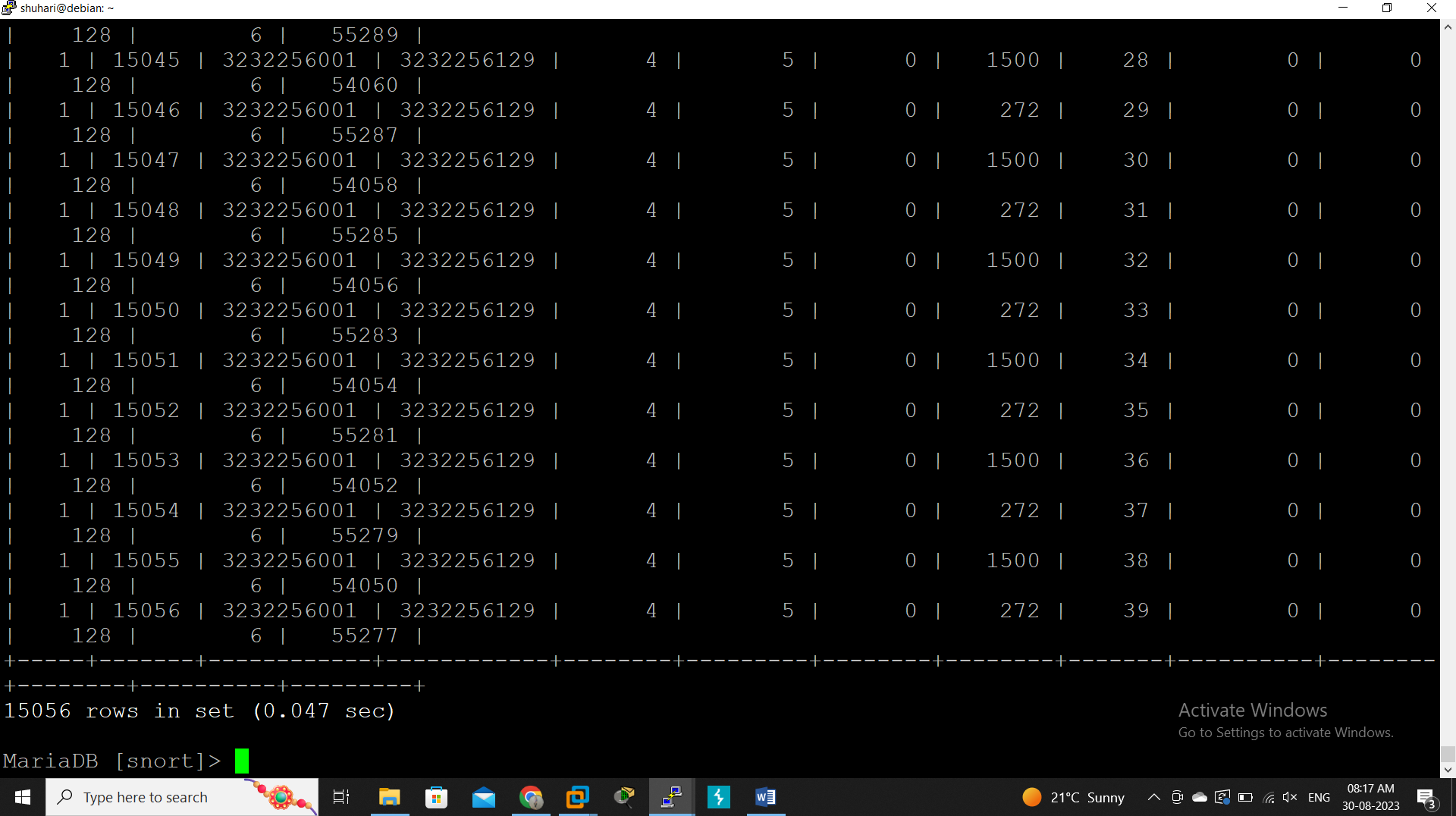
**/var/log/snort/barnyard2.waldo –g snort –u snort**



## Sudo mysql –u root -p



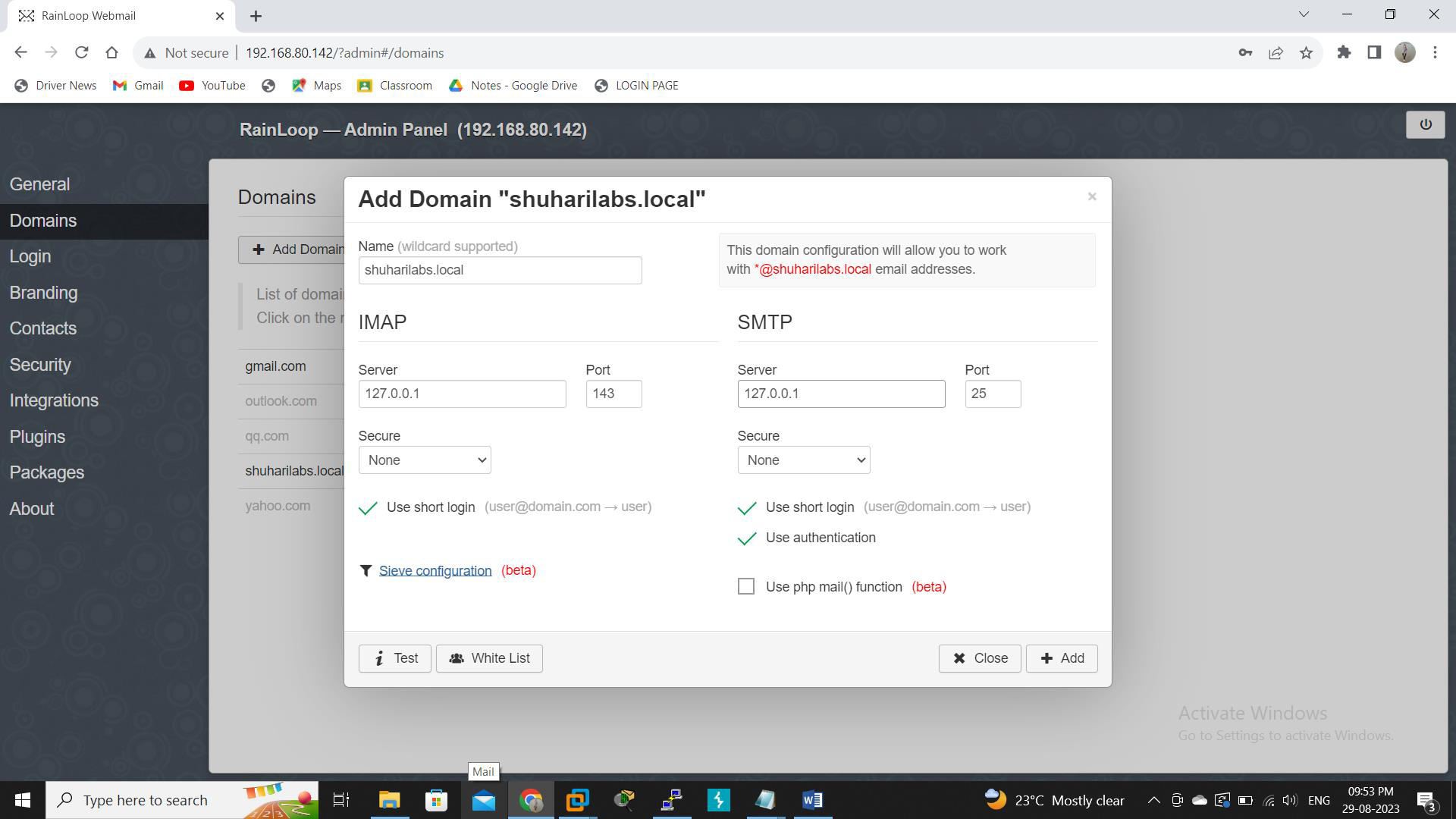
**MariaDB [snort]> select \*from iphdr;**

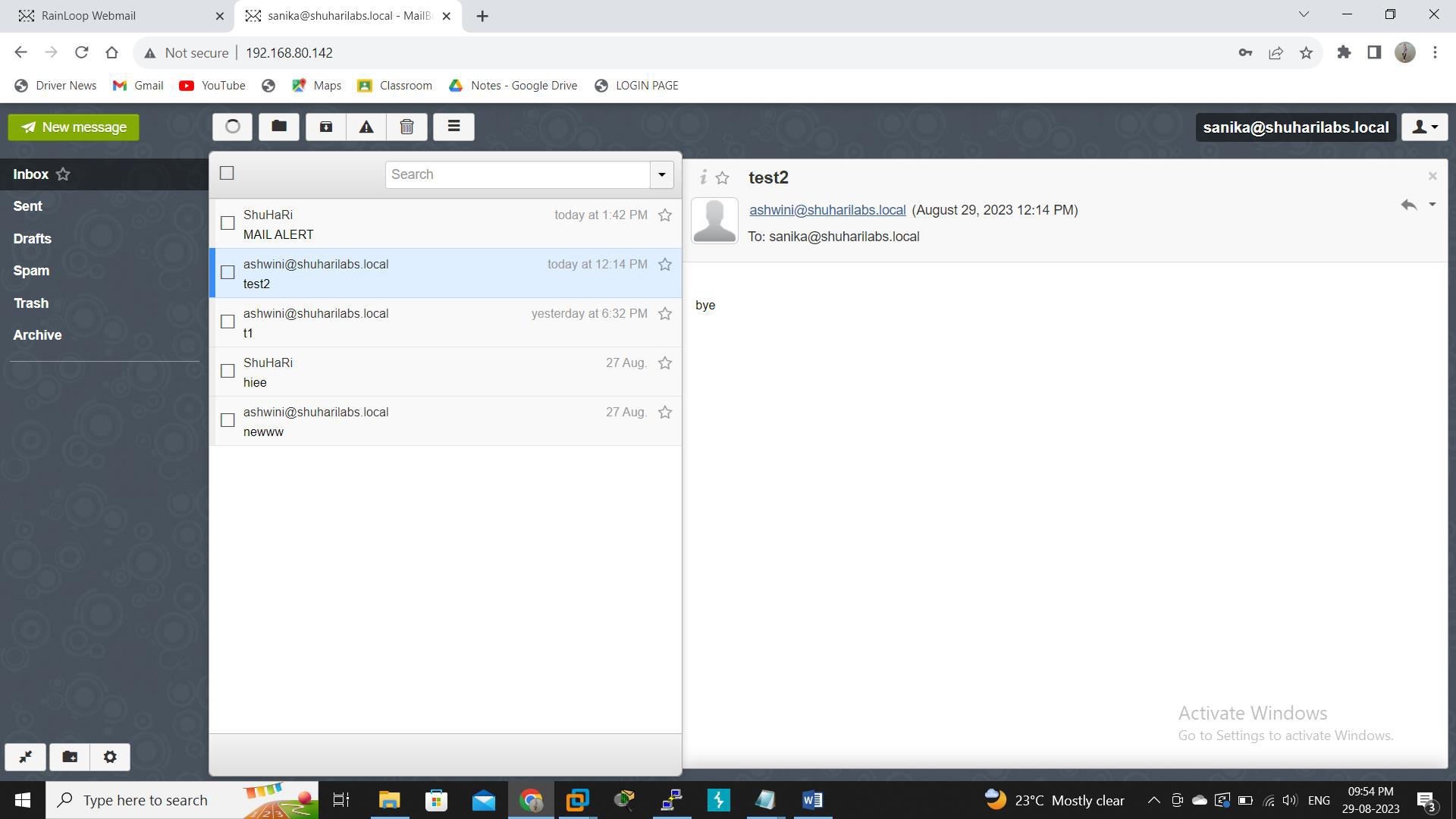


# SMTP Server

* + 1. **Test Configuration**

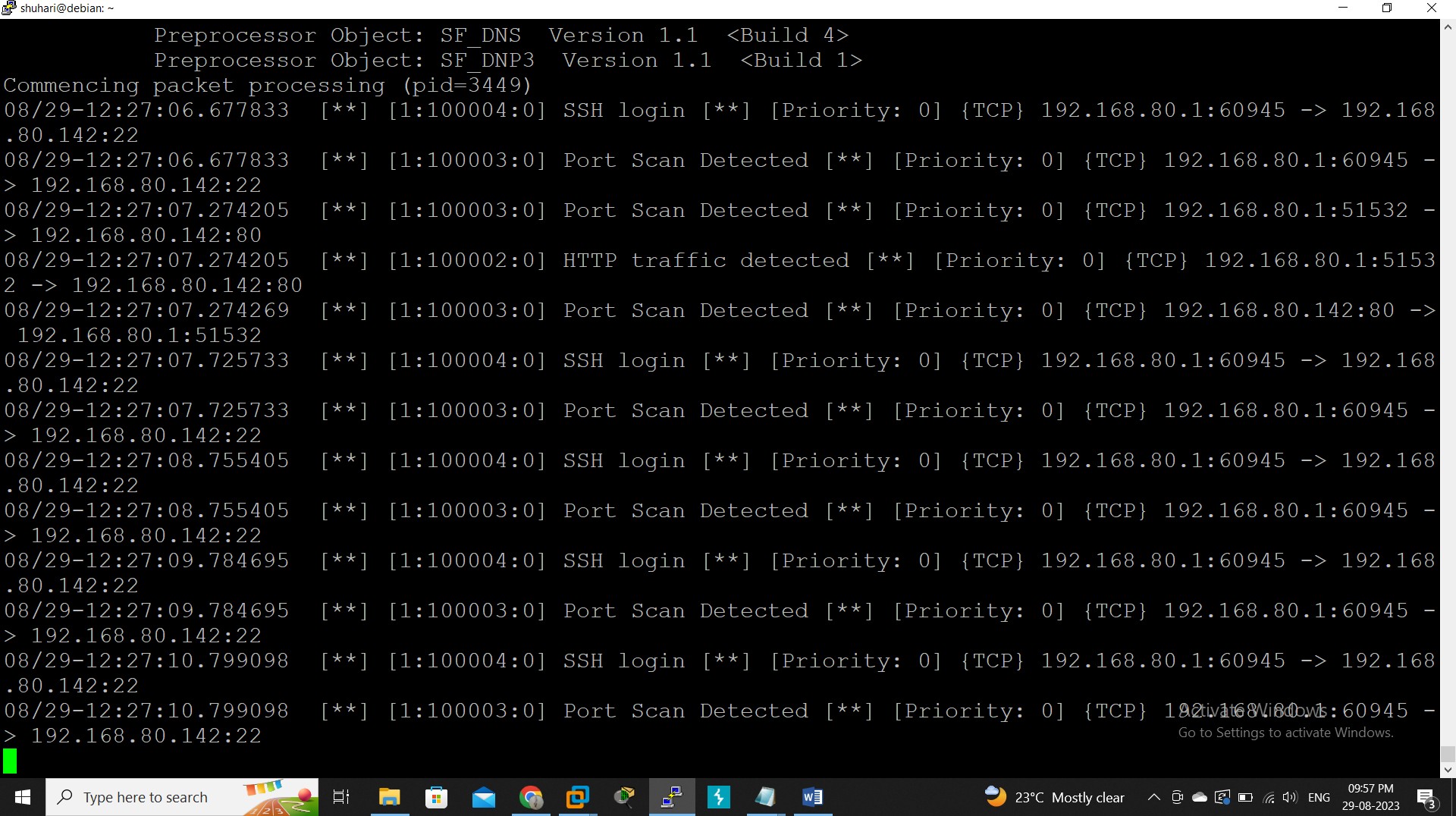




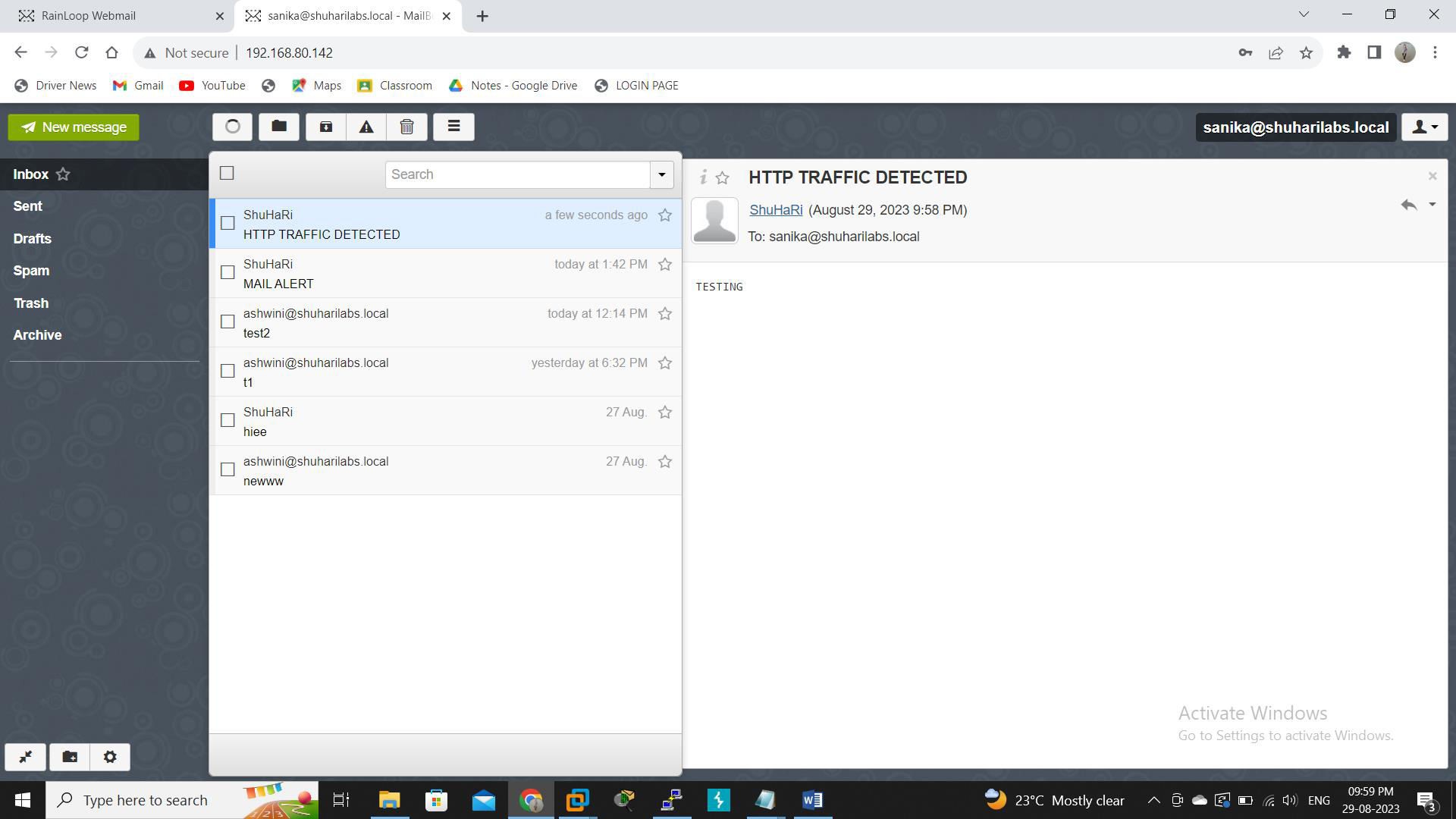


# Test Project

* + 1. **Detect Traffic**



# Email Alerts



1. **ADVANTAGES AND DISADVANTAGES**

# Advantages:

* **Real-Time Threat Detection**: Automated monitoring with Snort enables real-time detection of intrusion attempts, unauthorized access, and suspicious activities. This allows for immediate response to potential threats as they occur.
* **Immediate Notifications**: Email alerts provide instant notifications to administrators and security personnel when a security event is detected. This enables swift action to be taken to mitigate risks and prevent potential breaches.
* **Reduced Downtime**: Timely alerts allow administrators to respond quickly to security incidents, reducing the potential impact and minimizing downtime associated with breaches or attacks.
* **Efficient Resource Allocation**: Automated alerts eliminate the need for constant manual monitoring, freeing up security personnel to focus on more strategic tasks, such as incident analysis and response planning.

# Disadvantages:

* **False Positives and Negatives:** Automated systems, including Snort, can generate false positives (incorrectly identifying legitimate traffic as malicious) or false negatives (failing to detect actual threats). This can lead to alert fatigue and reduced trust in the system's accuracy.
* **Configuration Complexity:** Configuring Snort and related tools can be complex, especially for users with limited technical expertise. Misconfigurations may lead to improper alerting, missed threats, or performance issues.
* **Email Overload:** Depending solely on email alerts for intrusion detection can result in a flood of notifications, overwhelming administrators and causing them to miss critical alerts amidst the noise.
* **Latency in Alerting:** While email alerts are faster than manual monitoring, there can still be a delay between detecting an intrusion and receiving an alert. This delay could allow attackers to exploit vulnerabilities before actions are taken.

# 8. CONCLUSION

In summary, the project "Automated Intrusion Monitoring with Snort via Mail Alerts" has effectively combined the power of Snort intrusion detection with automated email alerts to create a robust security solution. This project provides real-time threat detection and immediate notification, empowering administrators to respond swiftly and prevent potential breaches. By seamlessly integrating these technologies, the project contributes to enhancing network security and for tifying defenses against Emergingcy berthreats.

1. **REFERENCE**

* *Barnyard2* [*https://github.com/firnsy/barnyard2/blob/master/doc/README.database*](https://github.com/firnsy/barnyard2/blob/master/doc/README.database)
* *Snort Manual*

[*http://manual-snort-org.s3-website-us-east-1.amazonaws.com/*](http://manual-snort-org.s3-website-us-east-1.amazonaws.com/)

* *SMTP Server*

[*https://sendgrid.com/blog/what-is-an-smtp-server/*](https://sendgrid.com/blog/what-is-an-smtp-server/)

* *Email Alerts*

[*https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-*](https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications)[*notifications*](https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications)

* *DNS*

[*https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-top*](https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-top)

* *MariaDB* [*https://mariadb.com/kb/en/documentation/*](https://mariadb.com/kb/en/documentation/)