1. **Project Title-** Spam Mail Detection

2. **Project Description-**

Email Spam is the electronic version of junk mail. It involves sending unwanted messages,often unsolicited advertising, to a large number of recipients. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks. In this we will be detecting spam mails of the user.

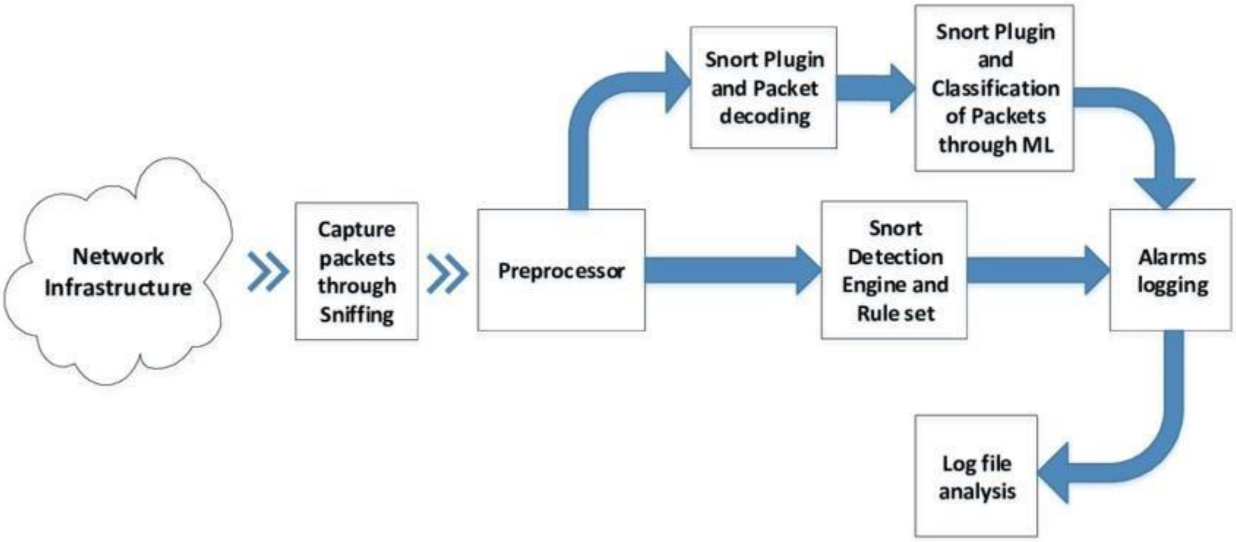
3. **Tools-** Snort

4. **Application of Tools in the project with a neat sketch**

   - Snort

Snort is a network intrusion detection system (NIDS) that can detect spam patterns. To use it effectively, custom rules need to be created to identify spam-related network traffic. These rules can look for specific SMTP commands, suspicious email headers, or unusual SMTP commands.

Snort's SMTP preprocessor can analyze SMTP traffic for anomalies or signs of spam activity. Content matching capabilities can search for specific patterns within email traffic. Flow analysis can identify patterns or anomalies indicative of spam activity. Snort can be integrated with other tools like SpamAssassin or ClamAV to enhance spam detection capabilities. However, it may not provide the same level of granularity and accuracy as dedicated spam filtering solutions.


Network Infrastructure
Capture packets through Sniffing
Preprocessor
Snort Plugin and Packet decoding
Snort Plugin and Classification of Packets through ML
Snort Detection Engine and Rule set
Alarms logging
Log file analysis

5. Expected outcome

- Comprehensive Analysis: By combining Wireshark's detailed packet capture and analysis with Snort's rule-based detection, we get a more comprehensive understanding of email traffic behavior and potential threats.
- Enhanced Detection: Wireshark provides granular visibility into email traffic, while Snort enhances detection with its rule-based approach, allowing identification of known spam patterns or malicious activities.
- Correlation of Events: Alerts generated by Snort can be correlated with specific email packets captured by Wireshark, providing context and aiding in incident response.
- Improved Response: The combined output enables faster detection and response to email-related security incidents, helping mitigate risks associated with spam, phishing, or malware distribution.