**Name: Dhaval Patel**

**Msc cyber security**

**Install and configure snort for**

**network security and protection**

**against cyber threats.**

Title: Installation and Configuration of Snort for Network Security and Protection Against Cyber Threats

Objective: To install and configure Snort, an open-source intrusion detection and prevention system (IDS/IPS), for network security and protection against cyber threats.

Requirements:

System running a compatible operating system (e.g., Windows, Linux).

Administrative privileges to install and configure software.

Procedures/Experimental Setup:

Download the latest version of Snort from the official Snort website or a trusted source.

Run the downloaded setup file to initiate the installation process.

Follow the on-screen instructions to install Snort on your system.

During the installation, choose the desired components and configurations based on your network requirements (e.g., IDS/IPS mode, network interfaces to monitor).

Configure the network interfaces to monitor by editing Snort's configuration file, usually located in the Snort installation directory.

Define the rulesets to use for detecting and preventing network intrusions. Snort provides both community and commercial rulesets that can be obtained from the Snort website or other trusted sources.

Customize the rule settings based on your network environment and security needs, such as enabling specific rules or modifying rule thresholds.

Set up logging and alerting mechanisms to capture and notify about potential security events. Configure Snort to send alerts to a central logging server or log events locally.

Start the Snort service or daemon to begin monitoring the network traffic and detecting potential threats.

Regularly monitor the Snort alerts and logs to identify and respond to detected threats.

Results:

Snort was successfully installed and configured on the system.

Network interfaces were set up for monitoring and detection.

Rulesets were configured to detect and prevent network intrusions.

Logging and alerting mechanisms were established to capture and notify about potential security events.

Snort service or daemon was started to monitor network traffic and detect threats.

Result Analysis:

With the installation and configuration of Snort, the system is now equipped to analyze network traffic and detect potential cyber threats.

Regular monitoring and analysis of Snort alerts and logs will help identify and respond to security incidents in a timely manner.

Conclusion:

The installation and configuration of Snort provide a robust network security solution with intrusion detection and prevention capabilities.

By customizing the rulesets and configuring logging/alerting mechanisms, the system can effectively detect and respond to potential cyber threats.

Regular maintenance and monitoring of Snort will contribute to a more secure network environment, protecting against various types of attacks.