2. Intrusion Detection Module: Develop an intrusion detection system to identify and respond to suspicious activities, including alerting or blocking.

#Background Research:

Understanding Intrusion Detection Systems (IDS):

- Researched and gained an understanding of the role and importance of Intrusion Detection Systems in network security.

Tool Selection:

- Explored different IDS tools and selected Snort as the preferred tool for intrusion detection. Considered its features, community support, and flexibility.

Installation and Configuration:

- Installed and configured Snort on the Parrot OS. This likely involved understanding system requirements, dependencies, and the basic setup process.

Rule Management with Snorpy:

- Explored the use of Snorpy, a tool for managing Snort rules. Customized rules to tailor the intrusion detection system to specific network requirements.

Rule Creation for ICMP and UDP:

- Created custom rules for detecting ICMP and UDP traffic. This involves specifying conditions or signatures that, when matched, trigger alerts.

Signature IDs and Messages:

- Implemented signature IDs and meaningful alert messages in the rules. It is for identifying the type of threat detected and facilitating a quick and accurate response.

Alerting Mechanism:

- Configured an alerting mechanism within Snort to notify the administrator or relevant personnel when suspicious activities are detected.

This is the video demonstration of the Intrusion Detection module:

intrusion_detection.mp4

#Observations:

Rule Customization Impact:

- I observed that customizing rules using Snorpy had a direct impact on the system's ability to detect specific types of traffic. This customization allowed me to tailor the intrusion detection system to the unique characteristics of my network.

Alert Clarity and Significance:

- The inclusion of signature IDs and meaningful alert messages proved to be crucial. These alerts provided clear information on the nature of the detected activity, aiding in quick identification and response.

Effective Detection of ICMP and UDP:

- Through practical testing scenarios, I found that the intrusion detection system effectively detected ICMP and UDP traffic based on the customized rules. This demonstrated the reliability of the rules in identifying specific threat patterns.

Timely Alerting Mechanism:

- The configured alerting mechanism worked as expected, providing timely notifications when suspicious activities were detected. This real-time alerting is essential for responding promptly to potential security incidents.

Responsiveness to Threats:

- The system's responsiveness to different threats, especially ICMP and UDP-based attacks, highlighted the importance of having a dynamic and adaptive intrusion detection system. This adaptability is crucial for staying ahead of evolving security threats.