Name: Janvi Upare

Batch- May (cyber security)

INTRUSION DETECTION SYSTEM USING SNORT

An Intrusion Detection System (IDS) is a vital component of cybersecurity designed to identify unauthorized access or breaches in computer networks or systems. IDS continuously monitors network traffic or system activities for suspicious behaviour and issues alerts when such activity is detected. There are primarily two types of IDS: Network-based IDS (NIDS), which monitors the entire network by analysing the packets traveling across it, and Host-based IDS (HIDS), which focuses on monitoring a specific host or device, detecting anomalies such as unauthorized file modifications or unexpected system behaviours. Additionally, Hybrid IDS combines both NIDS and HIDS to offer a comprehensive security solution. IDS employ two main detection methods: Signature-based detection, which compares network traffic against a database of known attack patterns (effective for known threats but ineffective for new, unknown threats), and Anomaly-based detection, which establishes a baseline of normal behaviour and flags deviations as potential threats (capable of detecting new threats but may produce false positives). The core functions of IDS include monitoring, alerting, logging, and reporting on detected threats and incidents. The primary benefits of implementing IDS are early threat detection, enabling swift responses to potential breaches, and providing logs and data for forensic analysis, which is essential for investigating security incidents. Furthermore, IDS help organizations comply with regulatory and compliance requirements by consistently monitoring and reporting security events. However, IDS have limitations, such as the potential for generating false positives, where non-malicious activities that deviate from the norm trigger alerts, and false negatives, where sophisticated or novel threats may go undetected. Despite these limitations, IDS remain a crucial tool in the cybersecurity arsenal, providing continuous vigilance against unauthorized access and potential security breaches.

Snort is a popular open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that is widely used in cybersecurity to detect and prevent network intrusions. Developed by Martin Roesch in 1998 and now maintained by Cisco, Snort uses a combination of signature-based detection, protocol analysis, and anomaly-based detection to monitor network traffic in real-time. It captures and analyzes packets traveling across the network to identify patterns indicative of malicious activity. Snort is highly configurable, allowing users to define custom rules to detect specific types of threats, making it a versatile tool for network security.

Using Snort involves several key steps:

1. Installation and Configuration: Snort can be installed on various operating systems, including Linux and Windows. After installation, users configure Snort by editing its configuration file (snort.conf), specifying the network interfaces to monitor, and setting up logging and alerting preferences.

2. Rule Sets: Snort relies on rule sets to detect malicious activity. These rules define the patterns to look for in network traffic. Users can download pre-defined rule sets from the Snort community or create custom rules tailored to their specific needs. Rules are written in a specific syntax that includes criteria such as source and destination IP addresses, ports, and the content of packets.

3. Running Snort: Once configured, Snort can be run in various modes. In IDS mode, snort monitors network traffic and generates alerts when it detects suspicious activity. In IPS mode, Snort not only detects but also takes action to block or mitigate the detected threats.

4. Monitoring and Analysis: Snort generates alerts and logs that can be viewed in real-time or analysed later. These logs provide detailed information about detected threats, including timestamps, source and destination IPs, and the specific rule that triggered the alert. Users can use tools like Snorby, BASE, or Splunk to visualize and analyze Snort data more effectively.

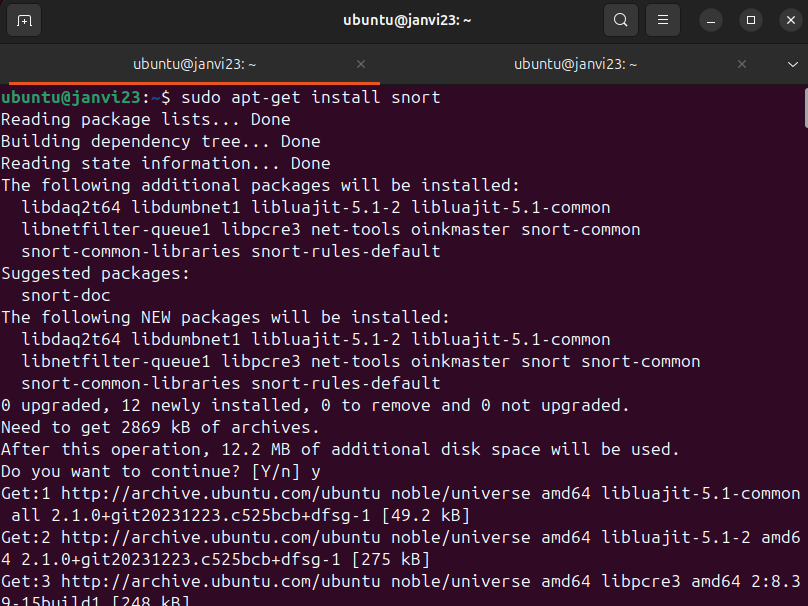
5. Regular Updates: Keeping Snort and its rule sets updated is crucial to maintaining effective protection against new and evolving threats. The Snort community and Cisco regularly release updates that include new rules and enhancements.

A diagram of a packet decoder

Description automatically generated

A diagram of a network

Description automatically generated



A screenshot of a computer

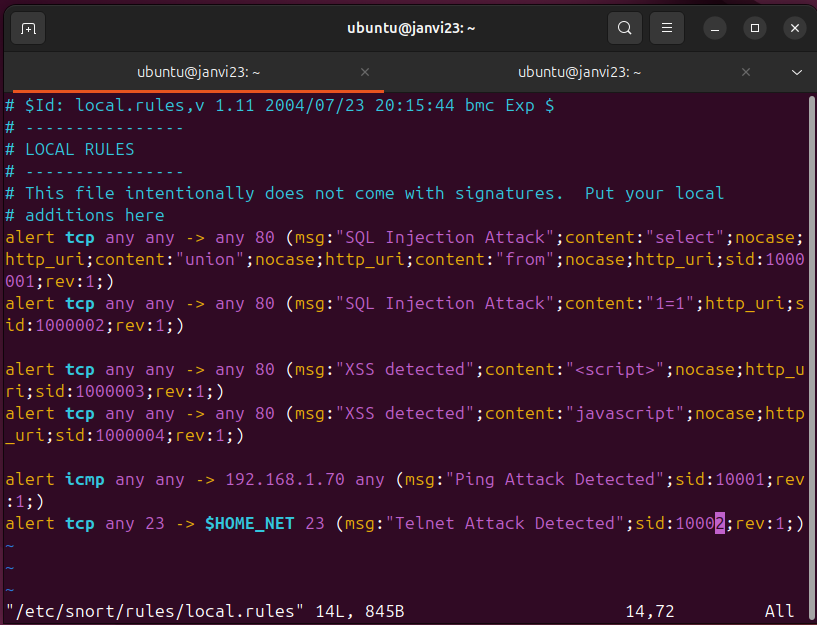
Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated