Ankush Singh
WorkShop_4

REPORT

Output Descriptions:

- **NO_NETWORK_POLICY:**
  When Kubernetes manifests without specifying network policies, there is a security misconfiguration. In a Kubernetes cluster, network rules are crucial for managing traffic flow between pods and services. Without them, every pod within a namespace is open to all network traffic, increasing the risk of unwanted access and security failures.

- **NO_ROLLING_UPDATE:**
  There is a security misconfiguration when Kubernetes appears without network policy specifications. Network rules are essential for controlling traffic flow between pods and services in a Kubernetes cluster. Without them, all network traffic may reach any pod inside a namespace, raising the possibility of unauthorized access and security failures.

- **INSECURE_HTTP:**
  The usage of HTTP instead of HTTPS for communication within or outside of the Kubernetes cluster is referred to as this misconfiguration. Due to HTTP's lack of encryption, data in transit is open to interceptions. To guarantee secure connection and safeguard sensitive data, HTTPS must be used.