**INTRODUCTION**

1. **Overview**

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An intrusion detection system can be a great tool for proactively monitoring and protecting your network from malicious activity, however they are also prone to false alarms.

An intrusion detection system (IDS) is a device that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Network security and security analysis level using Intrusion detection system are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use. Intrusion detection system for security and security analysis level for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. Network security and security analysis level using Intrusion detection system have become a necessary addition to the security infrastructure of nearly every organization.

Network security and security analysis level using Intrusion detection system typically record information related to observed events, notify security administrators of important observed events and produce reports. Many intrusion detection systems for security and security analysis level can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, ids tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. An ids installed on a network provides much the same purpose as a burglar alarm system installed in a house. Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert.

Although ids may be used in conjunction with firewalls, which aim to regulate and control the flow of information into and out of a network, the two security tools should not be considered the same thing. Using the previous example, firewalls can be thought of as a fence or a security guard placed in front of a house. They protect a network and attempt to prevent intrusions, while ids tools detect whether or not the network is under attack or has, in fact, been breached. Ids tools thus form an integral part of a thorough and complete security system. They don’t fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety.

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the ids will receive a notification of a possible security incident in the form of a page, email. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account.

**2. Objective**

* + Counter measure to detect or prevent attacks.
  + Know attack strategies.
  + Gather information which is then used to better identify, understand and protect against threats.
  + Divert hackers from productive systems.
  + SECURITY SERVER is primarily a research tool, but also has a real commercial application. The spoofing attack set in the server IP address on the adjacent, you will understand that it suffered the attack.
  + Reduce the data to be analyzed thus, data to identify the actual behavior of the attacker also much easier.