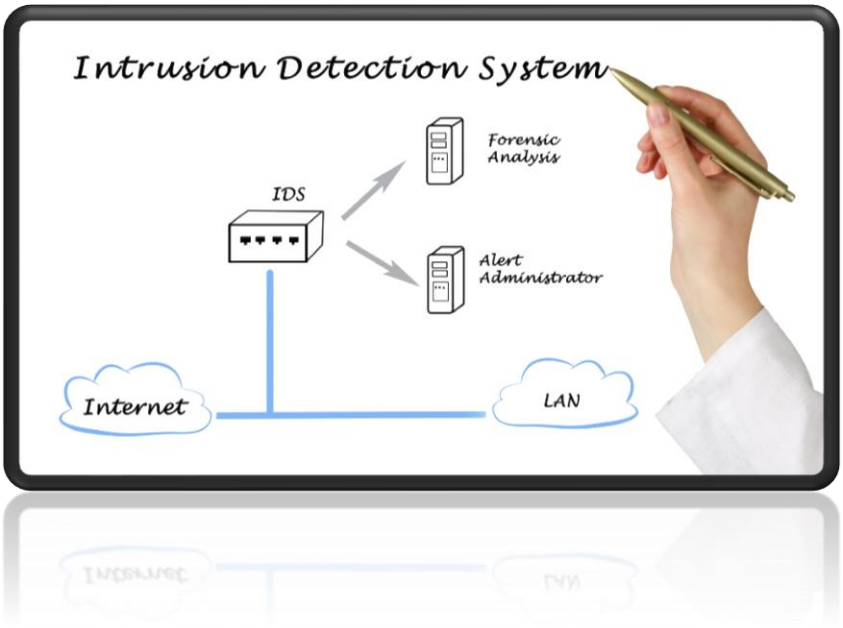
Assignment 2

Name: Divya Shah Branch: IT(T.E.) Roll No.:115 Date:30/09/2023

Q1 What is Intrusion Detection System? Explain different types of intrusion detection system with their working. State the advantages and limitations of each.

Solution –

An Intrusion Detection System (IDS) is a security technology that monitors network traffic or system events for signs of malicious activity or policy violations. IDSs are used to identify potential threats, log information about them, and report them to security administrators.



There are two main types of IDSs: **Network-based IDSs (NIDSs)** and **Host-based IDSs (HIDSs)**.

Network-based IDSs (NIDSs)

NIDSs monitor network traffic for signs of suspicious activity. They analyze network packets and look for patterns that match known attack signatures or other indicators of malicious behavior. NIDSs can be deployed at various points in a network, such as at the perimeter, within a subnet, or on individual hosts.

Host-based IDSs (HIDSs)

HIDSs monitor activity on individual hosts or endpoints. They analyze system logs, file integrity, and other host-specific data to detect signs of intrusion or compromise. HIDSs can be used to monitor servers, workstations, and other devices.

Advantages of NIDSs

- Can monitor large amounts of traffic across multiple hosts.
- Can detect attacks that bypass perimeter defenses.
- Can identify attacks that originate from within the network.

Limitations of NIDSs

- Cannot detect attacks that do not traverse the monitored network segment.
- May generate false positives due to normal network activity.
- May miss attacks that use encrypted traffic or other evasion techniques.

Advantages of HIDSs

- Can detect attacks that target specific hosts or applications.
- Can provide detailed information about the attack and its impact.
- Can detect attacks that bypass network defenses.

Limitations of HIDSs

- May generate false positives due to normal system activity.
- May miss attacks that occur outside the scope of the host's monitoring capabilities.
- Can be resource-intensive and impact system performance.