NAME: KAMALPREET KAUR

STUDENT ID: 202106526

Summary of lesson 6.

A network security technology called an intrusion detection system (IDS) keeps an eye on devices and network traffic for known hostile activities, questionable activity, or infractions of security policies.

IDSs are classified according to the type of activity they watch over and where they are in a system.

Systems for detecting network intrusions (NIDSs) monitor all incoming and outgoing traffic to devices connected to the network. To detect any hostile traffic leaking through, network intrusion detection systems (NIDS) are positioned strategically throughout the network, frequently right behind firewalls at the network's edge.

Installed on a particular endpoint, such as a server, laptop, or router, are host intrusion detection systems, or HIDSs. Only that device's activities, including traffic to and from it, is monitored by the HIDS. Typically, a HIDS operates by periodically capturing snapshots of important operating system files and comparing them over time.

Server and device connection protocols are monitored by a protocol-based intrusion detection system (PIDS). Web servers frequently have PIDS installed to track HTTP and HTTPS connections.

At the application layer, an application protocol-based intrusion detection system (APIDS) keeps an eye on protocols unique to each application. To find SQL injections, an APIDS is frequently installed in the middle of a web server and an SQL database.