Omkar Gurav
BE IT
8048

Rajdhani
DATE / /

ICS Class Assignment 1 (Mapping CO2)

Write a short note on Intrusion Detection System.

→

- An Intrusion Detection System (IDS) is defined as, a software that helps to find out if a system is breached.

- IDS does not help to prevent the attacks unlike anti-virus. It is only a system that can gather system information & find out if everything looks alright or not.

- At a high level, IDS is needed for the following reasons:

  ① Defense in Depth
  ② Automate intrusion detection
  ③ Corrective actions

- Broadly speaking, IDS can be classified based on what it monitors & how it monitors.

- Based on what it monitors, IDS can be classified into Network-based IDS (NIDS) & Host-based IDS (HIDS).

ⓐ Network-based IDS:-

It evaluate intrusions from the networking side. They watch all network traffic as it reaches the various information systems. If there

are any alerting situations based on the network traffic analysis, it notifies the administrator to take the corrective actions.

ⓑ Host-based IDS:-

Host-based IDS are typically installed on the individual information systems & then they watch for suspicious activities occuring on the system. System entities such as system services & processes etc are closely monitored to detect any undesired activities.

- Based on how it monitors, IDS can be classified into signature-based and Anomaly-based.

ⓐ Signature-based:-

Signature-based IDS has a pre-loaded database of various attack signatures. When it watches the activities, it constantly compares the activities patterns with that in the database. If a match is found, it raises an alert.

ⓑ Anomaly-based:-

Anomaly-based IDS first establishes the baseline of activities. It might take up to 2-3 weeks to "learn" what's right for a system. Once the learning phase is over, it would watch

out for any activities that are not part of that baseline & raise alerts.

Limitations & challenges of IDS:-

1. Does not prevent attacks.
2. High rate of false alerts
3. Complex systems
4. Bypassing IDS