

Intrusion Detection and Intrusion prevention (ID/IP) Systems

Introduction Intrusion & current Threat scenario

A set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource)

There are two types of threats

- Internal threats - Internal threats occur when someone has authorized access to the network with either an account or physical access. Just as for external threats, the severity of an internal threat depends on the expertise of the attacker
- External threats - These types of threats are caused by from individuals working outside of a company who do not have authorized access to the computer systems or network.

There are two ways of protection mechanisms

- Intrusion Detection
- Intrusion Prevention

Introduction to IDS/IPS

IDS –A System that automatically identifying intrusion activities.

IPS - A System that automatically identifying and responding to intrusion activities.

IDS/IPS Approaches and Detection Techniques

There are three types of approaches is used in the IDS//IPS to secure network.

- Signature based - This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined
- Anomaly based- This method of detection baselines performance of average network traffic conditions
- Policy based - This method identifies intrusions according to define organization policy
- Protocol Analysis based - This method identifies deviation of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity

Detection techniques

- State-less - They typically monitor and analyze all traffic in real-time on a packet-by-packet basis against a database of known patterns for a match
- State-full - A State-full IDS can be defined as a packet filtering and analysis mechanism which makes decision on current packet AND information from previous packets
- Deep packet inspection - Deep packet inspection (DPI) is an advanced method of packet filtering that functions at the Application layer of the OSI (Open Systems Interconnection) reference model.

Introduction of UTM

Unified threat management (UTM) refers to a comprehensive security product that includes protection against multiple threats

Advantages of UTM

- Simplicity
- Streamlined installation and use
- Ability to update all the security functions or programs concurrently
- Eliminates the need for systems administrators to maintain multiple security programs over time

Disadvantages OF UTM

- UTM introduces a single point of failure it lead for all the network security elements
- There is always a possibility of performance constraint as there are limitations in hardware processing capabilities to handle so many applications/users simultaneously
- There is always challenge from cloud computing initiatives and UTM's might have to be deployed in a virtual manner