INSTITUTO TECNOLOGICO DE CANCUN

LEON QUEB MIGUEL ANGEL

ISMAEL JIMENEZ SANCHEZ

FUND. TELECOMUNICACIONES

HORARIO

17:00 – 18:00

IDS/IPS

-Definición de IDS (Intrusion Detection System)

El IDS es un sistema que permite la detección de intrusos a una red, este posee sensores que permiten obtener datos. Con lo cual el sistema IDS puede detectar anomalías en el tráfico de red. La forma en la que funciona este sistema es analizando a detalle el tráfico de red, para que el IDS tenga un buen funcionamiento se debe usar junto a un Firewall ya que, por si solo un IDS no tiene la capacidad de detener un ataque.

-Definición de IPS (Intrusion Prevention System)

Se encarga de controlar el acceso a usuarios no registrados, con la posibilidad de poder bloquearlos. Para hacerlo puede usar distintas herramientas ya sea Hardware, Software o una combinación de ambas.

Según la forma de detectar ataques se categorizan en:

 Basado en firmas: compara el tráfico con firmas de ataques conocidos.

 Basado en políticas: como lo indica su nombre, se definen políticas estrictas.

 Basado en anomalías: método menos fiable ya que da muchos falsos positivos, para este método se encuentran dos opciones.

 Detección estadística de anormalidades: analiza el tráfico en un lapso de tiempo, después crea una lista de lo “normal”, posteriormente si el comportamiento varía mucho se considera la posibilidad de un ataque.

 Detección no estadística de anormalidades: para esta opción, el encargado de definir lo “normal” es el administrador del sistema.