IDS and IPS

04 February 2024 16:17

Three most important netsec devices – Firewalls – ✓
IDS
IPS

IDS – (Intrusion Detection System) – IDS monitors and alert if any intrusion (or) malicious activity is detected?
IPS – Intrusion Prevention System

Alarm

IDS – Alarm System – Monitor all the traffic
Fire Alarm
{Inspect} Detection techniques.
Attack
IPS – Sprinkler – Stop the fire
If it finds any intrusion – Report – Raise an Alarm
IDS
Past
ICMP Flood

How will it detect malicious activity Network attack
Signature

1) Signature based IDS
↓ Network Attack
Knowledge – based
Database

2) Anomaly based IDS
Ordinary behaviour
(out of the usual) un-usual
Data
100 ICMP (or) 100 SYN packets

Network Activity
– 50 ICMP packets

IDS – Detection and Raising the alarm

Behaviour – Based
ML
IPS
(New)
ML – Based
Zero-day
Statistics

Data
Malicious
Non-Malicious Data
Statistics
classification
Statistics

Not Block the Malicious act
Behaviour – ML
Machine Learning
Firewalls – stateful
IDS

Detection of classification
Machine Learning

Detection and Notification – {Not Block the attack, Notify} ↔ IPS
Active IDS
IPS ↔
Intrusion Prevention Prevention

IDS – Firewalls
NIDS → Network level (Router)
HIDS ↔ End point Security
Each and every host

IDS
Monitor
Alert

IDS / IPS
↓ Notify
↓ Blocks / Prevents the attack
Fundamental diff. b/w IDS and IPS

↓ ↓ Fundamental diff. b/w IDS and IPS

Notify — Blocks / Prevents the attack

IDS — Passive IDS - Normal - Notifies.

Classification
- How
  - Si Knowledge — signature-Based
  - Behaviour — Anomaly
- Where is it implemented?
  - NETWORK BASED — Routers & other switches.
  - Host BASED — End point security
- Reaction/Action
  - Passive IDS — Alert / Not block
  - Active IDS (IPS) — Alert / Block

Firewall classification

How
- Stateless — Packet Inspection Firewall
- Stateful — Stateful Inspection Firewall

Basis (where is it implemented)
- Host based
- Network based
- Personal firewalls
- Cloud based firewall

9:45 PM