Snort

Intrusion Detection System (IDS)

- passive monitoring solution for detecting possible malicious activities/patterns, abnormal incidents, and policy violations

Main two types of IDS

- Network IDS (NIDS): monitors the traffic flow from various areas of the network. If a signature is identified, an alert is created
- Host-Based IDS (HIDS): monitors the traffic flow from a single endpoint device.

Intrusion Prevention System (IPS)

- active protection solution. It is responsible for stopping/preventing/terminating

Main two types of IPS

- Network IPS (NIPS): if a signature is identified, the connection is terminated

- Behaviour-based IPS (Network Behaviour Analysis - NBA)
  - the aim is to protect the traffic on the entire subnet.

The Network-Behavior Analysis System works similar to NIPS

Difference: Behaviour-Based systems require a training period.

- Wireless IPS (WISP): monitors the traffic flow a wireless network. It terminates the connection

- Host-Based IPS (HIPS): protects a single endpoint device. It terminates.

Techniques

Signature Based → relies on rules that identify the specific patterns of the known Behaviour

Behaviour Based → identifies new threats with new patterns that pass through signatures.
A model compares known/normal Behaviours with unknown/abnormal Behaviours

Policy-Based → compares detected activities with system configuration and security policies.

Snort has 3 primary uses:

- As a packet sniffer like tcpdump, as a packet logger, which is useful for network traffic debugging or can be used as a full-blown network IPS.

Capabilities of Snort:

- live traffic analysis
- Attack and probe detection
- Packet logging
- Protocol analysis
- Real-time alerting
- Modules & plugins
- Pre-processors
- Cross-platform support

Snort Modes:

- Sniffer Mode: Read and prompt IP packets
- Packet Logger Mode: Log all IP packets
- NIDS and NIPS modes

Snort initial

Parameters	Description
-v, --version	instance version
-c	Identifying the configuration file
-T	self-test, allows us to test our setup
-q	quiet mode prevents from displaying the default banner

Operation Mode 1 : Sniffer Mode

-v : VerBose. Display the TCP/IP output in the console

-d : Display the packet data (payload)

-e : Display the link-layer (TCP/IP/UDP/ICMP) headers

-X : Display the full packet details in HEX

-i : Helps define a specific network interface to listen to& or sniff.

sudo snort -v -i eth0

- sniff on the interface named "eth0". Once we simulate the parameter -v, it will autbmatically use the "eth0" interface.