Network based intrusion prevention system (nips)

Technology, Computer

Network Based Intrusion Prevention System (NIPS) Definition: An intrusion prevention system sit in-line on the network and monitors the traffic, and when a suspicious event occurs it takes action based on certain prescribed rules. An IPS is an active and real time device, unlike an Intrusion detection system which is not inline and they are passive devices. Intrusion prevention systems are considered to be the evolution of intrusion detection system. Alternately, an Intrusion prevention system is usually a hardware device that is connected to the network.

It function is to monitor the network for nay unwanted behavior and to prevent such behavior. A Network based Intrusion prevention system (NIPS) is used to monitor the network as well as protect the confidentiality, integrity and availability of a network. Its main functions include protecting the network from Threats such as Denial OF Service and unauthorized usage. Explanation: Network based intrusion Prevention system monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity. NIPS once installed in a network it is used to create Physical security zones.

This in essence makes the network intelligent and it and quickly discerns good traffic from bad traffic. In other words the NIPS becomes like a prison for hostile traffic such as Trojans, worms viruses and polymorphic threats. NIPS are manufactured using high speed Application Specific Integrated Circuits (ASICS) and network processors. A Network processor is different when compared to a micro processor. Network processors are used for high speed network traffic, since they are designed to execute tens of thousands

of instructions and comparisons in parallel unlike a microprocessor which executes an instruction at a time.

NIPS are considered to be extensions of the present Firewall technologies. Firewalls inspect only the first four layers of the OSI model of any packet of information flow. However, NIPS inspects all seven layers of the OSI model making it extremely difficult to hide anything in the last four layers of a packet. Majority of the network based Intrusion prevention Systems utilize one of the three detection methods they are as follows: •Signature based detection: Signatures are attack patterns which are predetermined and also preconfigured.

This kind of detection method monitors the network traffic and compares with the preconfigured signatures so as to find a match. On successfully locating a match the NIPS take the next appropriate action. This type of detection fails to identify zero day error threats. However, it has proved to be very good against single packet attacks. •Anomaly based detection: This method of detection creates a baseline on average network conditions. Once a baseline has been created, the system intermittently samples network traffic on the basis of statistical analyses and compares the sample to the created baseline.

If the activity is found to be outside the baseline parameters, the NIPS takes the necessary action. •Protocol State Analysis Detection: This type of detection method identifies deviations of protocol states by comparing observed events with predefined profiles. Comparison OF NIPS andHIPS: Network Based intrusion prevention System: •Monitors and analyzes all the network activities. •Easier to setup, understand and implement. •It proves to

be better in detecting and preventing attacks or suspicious activities from the outside. •Less expensive. Near real-time response. Host based intrusion Prevention System: •Narrow in scope, watches only certain host activities. •Much more complex setup and understanding when compared to NIPS. •Better in detecting and preventing attacks from the inside. •More expensive than NIPS. Comparison OF NIPS and NIDS: Network Based Intrusion Prevention System: •Acts as a network gateway. •Stops and checks suspicious packets. •Prevents successful intrusions. •False positives are very bad. Network Based Intrusion Detection System: •Unlike NIPS, it only observes network traffic. NIDS logs suspicious activities and generates alerts. •Cannot stop an intruder, unlike NIPS. •False positives are not as big an issue when compared to network based intrusion prevention system. Summary: A Network based intrusion prevention system must meet the very basics necessities of networking. They are as follows: •Low latency: Less than 3ms, regardless of frame size, traffic mix, line rate or attack filter count. •Large session counts: Around 50, 000 to 1, 00, 000 simultaneous sessions. •Multi-Gigabit Speeds: To support backbone traffic and protect against internal attack. High availability: Must automatically become a transparent switch should any internal element collapse. •Precision: Should neither block nor drop good traffic. Sources: http://www. cisco. com/web/about/ciscoitatwork/security/csirt_network-based_intrusion_prevention_system. html http://en. wikipedia. org/wiki/Intrusion_prevention_system http://www. foursquareinnovations. co. uk/software_development_and_ebusiness_articles/intrusion_prevention_syste

ms_5. html http://www. infosecwriters. com/text_resources/pdf/JCooper_NIPS. pdf