What it is Network intrusion detection system?

combofix.org/what-it-is-network-intrusion-detection-system.php

To understand what is a network intrusion detection system one should first know what intrusion is. When a hacker tries to make way into your system, it is known as intrusion, and a network intrusion detection system is a system, which detects such intrusions. The word network is used for this system, because it keeps an eye on packets on a network wire and its main objective is to find out whether a cracker or a hacker is breaking into your system. It analyzes the traffic on your network to monitor signs of different malicious activity.

Main objectives and functions of such systems

The main functions of a network intrusion detection system include:

- Detecting attacks: such a system detects security threats and attacks as and when they happen by providing real-time network monitoring.
- Offer information: If this system detects an attack, then it put forward information about the attack.
- Take corrective steps: Once an attack is detected by the system, the active systems also take measure to tackle the attack.
- Storage: It also stores the events either locally or otherwise in case of an attack.

Perimeter network is a good place for establishing such a system.

Primary types of network intrusion detection system

A network intrusion detection system is mostly place at strategic points in a network, so that it can monitor the traffic travelling to or from different devices on that network. While choosing such a system, you should compare the main types of a network intrusion detection system. There are mainly two types of such system. One is signature based system and the other is anomaly based system. A signature based intrusion detection system is tuned towards a particular vulnerability, so it has less number of false positives (FP), whereas anomaly based system will search for attacks that are out of the norms, leading to higher rate of false positives. Therefore, you should choose a system as per your specific requirements.

Pros of the system

The main benefits of a network intrusion detection system include:

- Easy deployment: Deploying such a system is easier, as you will not have to change your existing infrastructure or system. This is because such systems are autonomous operating system.
- Less cost: These systems can be installed for all the network segments, so it eliminates the requirement of software at each host in a network segment lowering down the cost of ownership.
- Detecting attacks: these systems can easily detect attacks, which have escaped from the scanners of host-based sensors.
- Retain evidence: Such a system detect real-time intrusion, so it does give the attacker a chance for removing the evidence of such attack.

Cons to look for

Apart from the pros, there are some cons that come with network intrusion detection systems. These are:

- These system can collect a large number of alerts in a day, overloading your work
- FP alerts can also be very high, which leads to less confidence on alerts
- If you try to cut down FP rate, then this can affect NIDS reliability

- Tasks like analyzing and filtering has to be done manually