07.5 Intrusion Detection

Network Based (NIDS)

Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting. Examples of Network IDS:

- SNORT

Host Based (HIDS)

Often referred to as HIDS, host based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting. Examples of HIDS:

- OSSEC - Open Source Host-based Intrusion Detection System
- Tripwire
- AIDE - Advanced Intrusion Detection Environment
- Prelude Hybrid IDS

Statistical anomaly and signature-based IDSes

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline
A signature based IDS will monitor packets on the network and compare them against a database of signatur attributes from known malicious threats.

Physical (Physical IDS)

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as prevention systems as well. Examples of Physical intrusion detections are:

- Security Guards
- Security Cameras

- Access Control Systems (Card, Biometric)
- Firewalls
- Man Traps
- Motion Sensors

Comparison with firewalls[edit]

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and is another form of an application layer firewall.

Intrusion Prevention

Intrusion prevention follows the same process of gathering and identifying data and behavior, with the added ability to block (prevent) the activity. This can be done with Network, Host, and Physical intrusion detection systems.[1]Wikipedia: http://en.wikipedia.org/wiki/Intrusion_detection