- Intrusion Detection Systems -

Basics of IDS

The term **intrusion** refers to nearly any variety of network attack, including the *misuse, abuse,* and *unauthorized access* of resources. The generic term **Intrusion Detection** refers to a device that monitors traffic patterns or signatures to determine whether an attack is occurring.

Two types of devices can provide real-time monitoring, by capturing and analyzing packets:

- **IDS (Intrusion Detection System)** – intended to react *after* a network attack has been detected.
- **IPS (Intrusion Prevention System)** – intended to react *before* the network attack compromises a system.

IDS/IPS technology is implemented using **network sensors**, which perform the real-time monitoring. If multiple-sensors are employed, a **centralized management station** is used to monitor/control all sensors. Sensors generally come in two forms: **hardware appliances** or **software**.

A key consideration is the *placement* of the sensors, to maximize efficiency and coverage. Common places to install a sensor would include:

- *Outside* the firewall (the *untrusted* side)
- *Behind* the firewall (the *trusted* side)
- On each network segment
- On critical hosts/servers (a *software* sensor)

IDS sensors can be placed **inline**, which forces all traffic to traverse *through* the sensor. This allows the IDS to monitor all traffic; however, the sensor also introduces an additional bottleneck and point-of-failure on the network.

Capturing and monitoring all packets on a network segment can be difficult, especially in a **switched** environment, as a switch will intelligently forward frames to only the appropriate port(s). This is opposed to a hub, which forwards all frames out all ports.

Higher-end switches support a feature called **port mirroring** (or **spanning**). This allows the traffic of one or more ports to be **copied** or **mirrored** to a destination port. This allows an IDS sensor to be placed on *only* the mirrored port, and still monitor all traffic on the switched segment.

* * *

IDS Response

IDS technologies require an accurate *profile* or *database* of what constitutes **normal traffic**, and what is considered **anomalous** traffic. This profile can be created one of several ways:

- **Manually** - by the network/security administrator.
- **Dynamically** – by allowing the IDS to create a baseline and then tune itself.
- **Externally** – by pointing the IDS to a centralized or public database of well-known vulnerabilities and attacks.

Anomalous traffic should **trigger** a **response** (usually called an **alarm**)**.** This response can take on many forms:

- **Notify –** sends an alarm to a centralized management device, email-address, phone number, etc.
- **Log –** stores information about alarm in a local log file or database.
- **Drop –** drops any offending packets.
- **Reset –** sends the TCP flag *RST* to an attacking host, to terminate the connection.
- **Block –** automatically blocks any new incoming connections from a suspected attacker.
- **Ignore** – performs no action.

An incomplete or inaccurate policy can lead to inconsistent alarms:

- **True Positive –** an alarm generated for a legitimate attack.
- **True Negative –** legitimate traffic that *does not* set off an alarm.
- **False Positive** – an alarm generated for legitimate traffic.
- **False Negative** – a legitimate attack that *does not* set off an alarm.

Obviously, a well-tuned IDS should minimize the number of **false negatives**. However, a large number of **false positives** can also be dangerous, as it may lead to a lax response from the network/security administrator.

* * *

IDS Products

Snort (http://www.snort.org/) is the most popular open-source IDS product available. It supports both Linux and Windows platforms. Snort is predominantly a command-line based interface, though a GUI front-end has been developed.

Common *commercial* IDS products include:

- Cisco Secure IDS
- ISS RealSecure
- Symantec IDS
- Checkpoint SmartDefense
- Computer Associates eTrust

Common IDS databases and resources:

- Distributed IDS Shield – http://www.dshield.org/
- Common Vulnerabilities and Exposures (CVE) - http://cve.mitre.org/

* * *