INTRUSION DETECTION SYSTEMS - A GENERAL OVERVIEW

Intrusion detection systems, or better known as IDS, are systems which can tell you about traffic.While you may question the worth of this, bear in mind that a firewall is simply a device which allows or disallows packets based upon what it's ruleset dictates, it does not actually detect attacks. Now an IDS does not detect actually detect attacks, but it does know the significance of the traffic it encounters. It does this by analyzing the data it see's and reporting anything which it deems to be worthy of interest or investigation.

Pattern Matching Mode
These systems function much like anti-virus software in that they use signature files against which they compare traffic. These signatures files contain the signatures of hundreds of attacks, and the IDS reports when it finds a match. Much like anti-virus software, these signature files need to be updated to recognize new attacks, but the cycle for this is a lot longer then it is for anti-virus scanners due to the fact that new attacks do not appear as often as new viruses.

Anomaly Detection Mode
These systems establish a baseline of traffic when they are first installed, and this baseline is used as the guideline for what "normal" traffic looks like. Any future deviation from this baseline is noted for investigation. This type of operation is useful in that it can detect new types of attacks, but the drawback is that the establishment of the baseline must be done properly in order for it to be any good. Also many legitimate changes to the network will alter the baseline, so it needs to be updated in order to function properly again.

The two modes above are ways in which an IDS attempts to find attacks, the following are a broad classification of the two types of IDS there are;

Network-Based IDS
This type of IDS is used to monitor network traffic in order to detect any attacks. Such an IDS can...

- Detect port scanning
- Detect spoofed packets
- Detect known attacks
- Detect trojan/backdoor traffic
- Report in real-time
- Has no impact on network performance

But the drawbacks of these types of IDS are..

- It cannot read encrypted traffic
- On a busy network it can miss packets
- Does not understand proprietary protocols
- It can only report on the traffic it can see
- Cannot report on changes made to specific machines

Host-Based IDS
This type of IDS is used to monitor a specific network machine and what happens on that machine. Instead of being worried about attacks seen on the network, this IDS is worried about who does what and what can happen on a machine. Such an IDS can...

- Detect failed logon attempts
- Changes to important files
- A user access a file to which he has no permissions
- A users gains privileges unexpectantly
- Be installed with no additional hardware
- Operate with encryption
- Detect whether an attack succeeded or failed

But the drawbacks of these types of IDS are...

- It cannot see network attacks
- Each installation must be customized
- Reports are not real-time
- The data it uses can require large amounts of storage
- Performance can suffer with it's use
- An attacker with unrestricted access can subvert it

Weaknesses
So how do attackers defeat systems that are specifically built to detect attacks? Well here are some of the common methods...

Overwhelm	An attacker sends so much data that the IDS just cannot examine all of it and some slips past unnoticed
Web text	An attackers uses URL character codes to trigger attacks rather then using normal text
Timeouts	An attacker slows down the attack so that each part of it is seen as unrelated to one another by the IDS
Extra Characters	The attacker simply puts extra characters into the attack in order to change the attack signature
Replace Spaces	An attacker uses "tabs" rather than spaces in the attack so as to change the attack signature
Reverse Attacks	An attacker basically runs the attack in reverse to confuse the IDS
Multiple Sessions	An attacker runs each step of the attack in a separate session
Multiple Sites	An attacker uses multiple points of origin to run the attack

Here finishes a general overview of Intrusion Detection Systems, do not be put of by the weaknesses I have listed here, an IDS is an important part of your overall security infrastructure. It can give you an important heads-up for an attacks which are busy getting started. So check them out, learn and have fun.