4.3 Implementing IDS

Many vendors supply IDSs. Each of these systems have their own strengths and weaknesses. Deciding which system is best for a particular environment depends on many factors, including the network environment, security level required, budget constraints, and the skill level of the person who will be working directly with the IDS.

4.3.1 Snort

Snort is perhaps the most well-known open source IDS available. It is a software implementation installed on a server to monitor incoming traffic. It typically works with a host-based firewall in a system in which both the firewall software and Snort run on the same machine. Snort is available for UNIX, Linux, Free BSD, and Windows. The software is free to download, and documentation is available at the website: www.snort.org. Snort works in one of three modes: **sniffer, packet logger, and network intrusion-detection**.

4.3.1.1 Sniffer

In packet sniffer mode, the console (shell or command prompt) displays a continuous stream of the contents of all packets coming across that machine. This can be a very useful tool for a network administrator. Finding out what traffic is traversing within a network can be the most efficient way to determine where potential problems lie. It is also a good way to check whether transmissions are encrypted.

4.3.1.2 Packet Logger

Packet logger mode is similar to sniffer mode. The difference is that the packet contents are written to a text file log rather than displayed in the console. This can be more useful for administrators who are scanning a large number of packets for specific items. Once the data is in a text file, users can scan for specific information using a word processor’s search capability.

4.3.1.3 Network Intrusion-Detection

In network intrusion-detection mode, Snort uses a heuristic approach to detecting anomalous traffic. This means it is rule-based and learns from experience. A set of rules initially governs the entire process. Over time, Snort combines what it finds with the settings to optimize performance. It then logs the traffic and can alert the network administrator. This mode requires the most configuration because the user can determine the rules that he/she wishes to implement for the scanning of packets. Snort works primarily from the command line (Shell in Unix/Linux, command prompt in Windows).

Configuring Snort is mostly a matter of knowing the correct commands to enter and understanding their output. Anyone with even moderate experience with either Linux shell commands or DOS commands can quickly master the Snort configuration commands. Snort is a good tool when used in conjunction with host-based firewalls or as an IDS on each server to provide additional security.

4.3.2 Cisco Intrusion Detection and Prevention

The Cisco brand is widely recognised and well respected in the networking profession. Along with their firewalls and routers, Cisco has several models of intrusion detection, each with a different focus/purpose. In the past, Cisco had two specific, widely used IDS products, the Cisco IDS 4200 Series Sensors and Cisco Catalyst 6500 Series Intrusion-Detection System (IDSM-2) Services Module.

There are a number of products in this group, notably the Firepower 4100 series, the Firepower 8000 series, and the Firepower 9000 series. All the products include malware protection as well as sandboxing. These Cisco products also integrate cyber threat intelligence features.

The 4100 series is targeted for small networks and the 9000 series is designed for large scale networks. One of the main benefits of using Cisco security products is their widespread use across the industry and the availability of good training. The fact that so many organisations use Cisco indicates a high level of successful field testing, which generally indicates a reliable product. Cisco also sponsors a range of certifications on its products, making it easier to determine whether someone is qualified on a particular Cisco product.