Chapter 15 Network Monitoring

Chapter Objectives

This chapter will discuss:

- Intrusion Detection Systems, which include:
- Inspectors,
- Honeypots/Honeywebs, and
- Auditors.

15.1 Monitoring the Network

With the amount of automated and human-generated attacks from around the Internet growing every day, the need to have an automated tool to evaluate what is and is not a threat worth reporting must be addressed. Intrusion Detection Systems (IDS) are the tool to detect, evaluate and block (or audit) the attacks. There are three main types of IDSs:

- Inspectors,
- Decoys, and
- Auditors

15.1.1 Inspectors

The inspector is the most common type of IDS, according to Strebe (2004), and are usually embedded within a firewall. They look for the following indicators of inappropriate use:

- Suspicious network traffic, such as port scans or connections to disallowed ports,
- "Telltales" of known attacks (such as worms or viruses),
- Spikes in resource utilization at unusual times, and
- File activity, such as creating new files, modifying system files or changing user accounts or security settings.

These occurrences are monitored and an audit trail is created for later inspection. Because an IDS relies on its catalog of known attacks, one that is unknown to it will not be detected and as such will not activate the report. Human inspection, therefore, is required as a supplement to the automated work and IDS is able to complete.

15.1.2 Decoys

Decoy IDSs, also known as *honeypots*, are built for the specific purpose of monitoring malicious activity. They "operate by mimicking the expressive behavior of a target system, except instead of providing an intrusion vector for the attacker, they alarm on any use at all. Decoys look just like a real target that hasn't been properly secured." (Strebe, 2004) A honeypot has been defined by the founder of the Honeynet Project as "a security resource whose value lies in being probed, attacked or compromised." (Chuvakin, 2003) The real value comes in the wealth of *by definition* malicious traffic information that is captured and available for analysis.

15.1.3 Auditors

As the name suggests, auditors create audit logs of what everyday users do in their jobs. This audit trail is available for analysis should the need arise. Some operating systems have built-in audit capabilities that can keep track of such things as password changes, spyware installation, changes to system files, etc. Some of the higher-end IDSs will also have the ability to inspect its logs for the telltale signs of an intrusion attempt. If, for example, the password for an admin's account is changed, a "red flag" will go up and a report will be issued to the administrator. (Strebe, 2004)

15.2 IDS' Relevance to the Enterprise

A key factor IDSs bring to the organization is that they allow what they have been programmed to consider to be normal network activity to pass through without note, but will at the very least detect and either passively audit the suspect activity or will actively alert the network administrator to the activity.

The true test comes in configuring the IDS, making sure it reports the correct amount of threats to the network administrators. Should there be such a huge volume of audit logs to be reviewed that it is impossible to do so the real value of the process is lost. As mentioned in the previous chapter, the normal business processes of the organization must be executed in