WHY USE AN IDS?

According to the NIST's documentation on industry best practices, there are several compelling reasons to acquire and use an IDS:

1. To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
2. To detect attacks and other security violations that are not prevented by other security measures
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other 'doorknob rattling' activities)
4. To document the existing threat to an organization.
5. To act as quality control for security design and administration, especially of large and complex enterprises.
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

One of the best reasons why organizations should install an IDS is that these systems can serve as straightforward deterrent measures, by increasing the fear of detection and discovery among would-be attackers. If internal and external users know that an organization has an intrusion detection system, they are less likely to probe or attempt to compromise it, just as criminals are much less likely to break into a house that has been clearly marked as having a burglar alarm.

The second reason for installing an 10S is to cover the organization when its network fails to protect itself against known vulnerabilities or is unable to respond to a rapidly changing threat environment There are many factors that can delay or undermine. An organization's ability to make its systems safe from attack and subsequent loss. For example, even though popular information security technologies such as scanning tools (to be discussed later in this chapter) allow security administrators to evaluate the readiness of their systems, they may still fail to detect or correct a known deficiency, or may perform the vulnerability-detection process too infrequently. In addition, even when a vulnerability is detected in a timely manner, it cannot

always be corrected quickly. Also, because such corrective measures usually involve the administrator installing patches and upgrades, they are subject to delays caused by fluctuation in the administrator's workload. To further complicate the matter, sometimes there are services that are known to be vulnerable, but they are so essential to ongoing operations that they cannot be disabled or otherwise protected in the short term. At such times-that is, when there is a known vulnerability or deficiency in the system-an IDS can be particularly effective, as it can be set up to detect attacks or attempts to exploit existing weaknesses. By, in effect, guarding these vulnerabilities, IDS can become an important part of the strategy of defense in depth.

The next reason why IDSs are useful is that they can help administrators detect the preambles to attacks. Most attacks begin with an organized and thorough probing of the organization's network environment and its defenses. This initial estimation of the defensive state of an organization's networks and systems is called doorknob rattling and is conducted first through activities collectively known as foot printing (which involves gathering information about the organization and its network activities and the subsequent process of identifying network assets), and then through another set of activities collectively known as fingerprinting (in which network locales are scanned for active systems, and then the network services offered by the host systems on that network are identified). When a system is capable of detecting the early warning signs of foot printing and fingerprinting, much as neighborhood watch volunteers might be capable of detecting potential burglars who ale casing their neighborhoods by skulking through and testing doors and windows, then the administrators may have time to prepare for a potential attack or to take actions to minimize potential losses from an attack.

A fourth reason for acquiring an IDS is documentation. In order to justify the expenses associated with implementing security technology like an IDS (and other controls such as firewalls), security professionals frequently have to make a business case. Since projects to deploy these technologies are often very expensive, almost all organizations require that project proponents document the threat from which the organization must be protected. The most frequent method used for doing this is to collect data on the attacks that are currently occurring in the organization and other similar organizations. While such data can be found in published reports or journal articles, first-hand measurements and analysis of the organization's own local network data are likely to be the most persuasive. As it happens, one means of collecting such

data is by using IDS. Thus, IDSs are self-justifying systems-that is, they can serve to document the scope of the threat(s) an organization faces and thus produce data that can help administrators persuade management that additional expenditures in information security technologies (e.g., IDSs) are not only warranted, but critical for the ongoing protection of information assets. Measuring attack information with a freeware IDS tool (such as snort) may be a way to begin this process of documentation.

Another reason that supports the use of an IDS relates to the concepts of quality assurance and continuous improvement, which are both we!! known to most senior managers. In terms of quality control, IDSs support the concept of defense in depth, for they can consistently pick up nformation about attacks that have successfully compromised the outer layers of information security controls--that is, compromised controls such as a firewall. This information can be used to identify and repair emergent or residual flaws in the security and network architectures, and thus help the organization expedite its incident response process and make other such continuous improvements.

A final reason for installing an IDS is that even if an IDS fails to prevent an intrusion, it can still assist in the after-attack review by helping a system administrator collect information on how the attack occurred, what the intruder accomplished, and which methods the attacker employed. This information can be used, as discussed in the preceding paragraph, to remedy deficiencies as well as trigger the improvement process to prepare the organization's network environment for future attacks. The IDS may also provide forensic information that may be useful as evidence, should the attacker be caught and criminal or civil legal proceedings pursued. In the case of handling forensic information, an organization should follow commonly accepted and legally mandated procedures for handling evidence. Foremost among these is that the information collected should be stored in a location and manner that precludes its subsequent modification. Other legal requirements and plans the organization has for the use of the data may warrant additional storage and handling constraints. As such, an organization may find it useful to consult with legal counsel when determining policy governing this situation.2