DEPLOYING HOST-BASED IDSS AND MEASURING THE EFFECTIVENESS OF IDSS

The proper implementation of HIDSs can be a painstaking and time-consuming task, as each HIDS must be custom configured to its host systems. Deployment begins with implementing the most critical systems first This poses a dilemma for the deployment team, since the first systems to be implemented are mission-critical and any problems in the installation could be catastrophic to the organization. As such, it may be beneficial to practice an implementation on one or more test servers configured on a network segment that resembles the mission-critical systems. Practicing will help the installation team gain experience and also help determine if the installation might trigger any unusual events. Gaining an edge on the learning curve by training on non-production systems will benefit the overall deployment process by reducing the risk of unforeseen complications.

Installation continues until either all systems are installed, or the organization reaches the planned degree of coverage it is willing to live with, with regard to the number of systems or percentage of network traffic. Lastly, to provide ease of management, control, and reporting, each HIDS should, as discussed earlier, be configured to interact with a central management console.

Just as technicians can install the HIDS in off-line systems to develop expertise and identify potential problems, users and managers can gain expertise and understanding of the operation of the HIDS by using a test facility. This test facility could use the off-line systems configured by the technicians, but also be connected to the organization's backbone to allow the HIDS to process actual network traffic. This setup WiIl also enable technicians to create a baseline of normal traffic for the organization. During the system testing process, training scenarios can be developed that will enable users to recognize and respond to common attack situations. Finally, to ensure effective and efficient operation, the management team can establish policy for the operation and monitoring of the HIDS.

Measuring the Effectiveness of IDSs

IDSs are evaluated using two dominant metrics: first, administrators evaluate the number of attacks detected in a known collection of probes; second, the administrators examine the level of use, commonly measured in megabits per second of network traffic, at which the IDSs fail. An evaluation of an IDS might read something like this: *at]00 Mb/s, the* IDS *was able* to *detect* 97% *of directed attacks.* This is a dramatic change from the previous method used for assessing IDS effectiveness, which was based on the total number of signatures the system was currently running-a sort of "more is better" approach. Unfortunately, this evaluation method of assessment was flawed for several reasons. Not all IDSs use simple signature-based detection. Some systems, as discussed earlier, can use the almost infinite combination of network performance characteristics of statistical-anomaly-based detection to detect a potential attack. Also, some more sophisticated signature-based systems actually use *fewer* signatures/rules than older, simpler versions-which, in direct contrast to the signature-based assessment method, suggests that less may actually be more. The recognition that the size of the signature base is an insufficient measure of an IDS' effectiveness led to the development of stress test measurements for evaluating IDS performance. These only work, however, if the administrator has a collection of known negative and positive actions that can be proven to elicit a desired response. Since developing this collection can be tedious, most IDS vendors provide testing mechanisms

that verify that their systems are performing as expected. Some of these testing processes will enable the administrator to:

- Record and retransmit packets from a real virus or worm scan
- Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
- Conduct a real virus or worm scan against an invulnerable system

This last measure is important, since future IDSs will probably include much more detailed information about the overall site configuration. According to experts in the field, "it may be necessary for the IDSs to be able to actively probe a potentially vulnerable machine, in order to either pre-load its configuration with correct information, or perform a retroactive assessment An IDS that performed some kind of actual system assessment would be a complete failure in today's generic testing labs, which focus on replaying attacks and scans against nonexistent machines.

With the rapid growth in technology, each new generation of IDSs will require new testing methodologies: However, the measured values that will continue to be of interest to IDS administrators and managers will, most certainly, include some assessment of how much traffic the IDS can handle, the numbers of false positives and false negatives it generates, and a measure of the IDSs ability to detect actual attacks. Vendors of IDSs systems could also include a report of the alarms sent and the relative accuracy of the system in correctly matching the alarm level to the true seriousness of the threat. Some planned metrics for IDSs may include the flexibility of signatures and detection policy customization.

IDS administrators may soon be able to purchase tools that test IDS effectiveness. Until these tools are available from a neutral third party, the diagnostics from the IDS vendors will always be suspect. No matter how reliable the vendor, no vendor would provide a test their system would fail.

One note of caution: there may be a strong tendency among IDS administrators to use common vulnerability assessment tools, like Nmap or Nessus, to evaluate the capabilities of an IDS. While this may seem like a good idea, it will in fact not work as expected, because most IDS systems are equipped to recognize the differences between a locally implemented vulnerability assessment tool and a true attack.

In order to perform a true assessment of the effectiveness of IDS systems, the test process should be as realistic as possible in its simulation of an actual event. This means coupling realistic traffic loads with realistic levels of attacks. One cannot expect an IDS to respond to a few packet probes as if they represent a denial-of-service attack. In one reported example, a program was used to create a synthetic load of network traffic made up of many TCP sessions, with each session consisting of a SYN (or synchronization) packet, a series of data, and ACK (or acknowledgement) packets, but 110 FIN or connection termination packets. Of the several IDS systems tested, one of them crashed due to lack of resources while it waited for the sessions to be closed. Another IDS passed the test with flying colors because it did not perform state tracking on the connections. Neither of the tested IDS systems worked as expected, but the one that didn't perform state tracking was able to stay operational and was, therefore, given a better score on the test.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf