Intrusion Detection

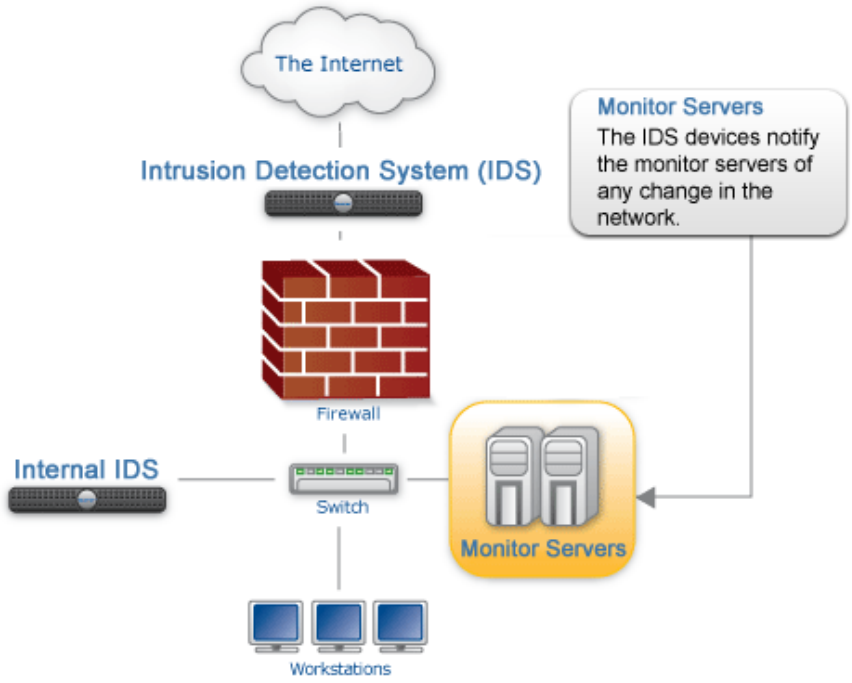
Marlicia J. Pollard
East Carolina University
ICTN 4040 SECTION 602
Mrs. Boahn
Dr. Lunsford

For this term paper I will be discussing the subject of Intrusion detection. I will be going in depth as to what steps one could take to prevent intrusions on their network and what different signs to look for if they think that an intrusion has occurred. There are two main types of Intrusion Detection Systems, which are Host based and Network based. There are many different pros and cons to both of these systems. Intrusion Detection Systems are being developed and constantly modified to try to stop and limit the amount of attacks on networks.

Intrusions are the activities that violate the security policy of systems and intrusion detection is the process used to identify intrusions. The concept was first born in 1980 by James Anderson. Every since 1983, SRI's International Computer Science Lab has been actively involved in intrusion detection. In 1984, Dr. Dorothy Denning and SRI actually developed the first model for Intrusion Detection, which was called The Intrusion Detection Expert System. The Haystack Project at the University of California Lab released the Intrusion Detection system for use to the United States Air Force in 1988. Intrusion Detections systems have been a major factor for a while now.

An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches and misuse. These possible breaches include, both attacks from outside the organization and attacks from with in the organization. The ID system uses vulnerability assessment. This assessment is sometimes referred to as scanning. It is a technology developed to assess the security of a computer system or network.

The IDS has many functions that are important in it's protection. With these functions it prepares for and deals with attacks by collecting information from a variety of system and network sources. Then it analyzes the symptoms of security problems. The IDS serve three essential security functions. These functions include monitor, detect and respond to unauthorized activity. In the function of monitoring the IDS monitors and analyzes both user and system activities. When analyzes it is searching for system configurations and vulnerabilities. After the vulnerabilities are detected then the system and file integrity is assessed. The system recognizes typical patterns of attacks and abnormal activity. It then tracks the violations and responds to any unauthorized activity automatically, in real time, to a security breach event. Logging off a user, disabling a user's account, and launching some scripts, can do this.



(In this figure, you can see the process of the Intrusion Detection System.)

Intrusion Detection systems are being developed because of the increasing amount of attacks on major sites and networks. Just to name a few are those of the US Defense Department, NATO, The White House and the Pentagon. Everyday networks have to face the possibility of having an attack against them and systems constantly have to be updated and monitored to avoid attacks that could cause a major loss. There are two procedures to Intrusion Detection Systems. The first is host based and is looked at to be the passive component. The host-based system inspects the system's configuration files to point out any unwise settings, inspects password files to look for passwords that could be easily figured out, and inspects other system areas to detect policy violations. The second is the network based which is looked at to be the active component. This process is basically run by known methods of attacks. It has a database that obtains known attacks and reenacts them to see how the system responds.

There are many benefits to the Intrusion Detection Systems. These include: monitoring the operation of firewalls, routers, key management servers and files critical to other security mechanism, allows administrators to tune, organize and understand operating system audit trails and other logs that aren't usually able to be understood, they provide a user friendly interface that can be used by individuals that aren't experts, they come with a very detailed attack signature database in which information from the customers system can be matched, and can recognize and report changes to data files.

Host Based Intrusion Detection Systems can get audit data from host audit trails and detect attacks against a single host. They work in switched network

environments and also operate in encrypted environments. They have the ability to detect and collect the most relevant information in the quickest possible manner. The host-based systems are also able to track behavior changes associated with misuse. The use of the resources of a host server like (disk space, RAM, and CPU time) is required by a host-based system. And lastly they do not protect the entire infrastructure. Host Based analyzes activities monitors at a high level of detail on the host. The system is able to tell which processes or users are involved in malicious activities on the network. Many host-based Intrusion detection systems use an agent-console model where agents monitor individual hosts but report to a single centralized console. They have the ability to detect attacks that are meant to be undetectable to network-based systems and access attack effects precisely. Host based systems use encryption services to look at encrypted traffic, data, storage, and activity. Being able to see encrypted data is major advantage because so many things can be hidden behind encrypted data. There are a few cons to host based systems, which include: data collection occurs on per host basis and attackers who are smarter than most could possibly disable a host based system. Host based systems take up a lot of processing time, storage, memory and other resources where systems operate which can also be a huge downfall.

Network based is another type of IDS. This system uses a passive interface to capture network packets for analyzing. Network sensors placed around the globe can be configured to report back to a central site, which enables a small team of security experts to support a large enterprise. This system scales well for network protection because the number of actual workstations servers or user systems on

the network is not really critical. It is more about the amount of traffic that is what really matters. Most of the Network based IDSs are CS independent. It also provides better security against DOS attacks.

The Network based system has both its pros and cons. On the pro side of the network, the IDS can monitor an entire, large network with only a few nodes or devises. The system is also mostly passive devises that monitor ongoing network activity without interring with network operation. They are easy to secure against an attack and may even be undetectable to hackers. The installation is easy and easier to use on an existing network. On the con side of the system the system cannot scan protocols or content if network traffic is encrypted. This is because Intrusion detection becomes more difficult on modern switched networks. Currently network based systems are based on a predefined attack signatures. These signatures will always be a step behind the latest underground exploits. May not be able to monitor and analyze all traffic on busy networks that are large. Network based IDS's require a certain amount of hands on involvement of network administrators.

Overall based from research and analysis Intrusion Detection System is a great idea to put into place to avoid unwanted people on an organization's network trying to steal information. The IDS is becoming the most logical next step after deploying firewall technology at the network perimeter. With any system it has it's pros and cons as discussed above, but the implementation of the IDS decreases the chances of attack drastically. The IDS system continues to grow and evolve to protect an organization from the attackers and to keep their information safe.

Bibliography

Snort---The open source intrusion detection system. (2002). Retrieved March 7, 2015, from http://www.snort.org

An Introduction To Intrusion Detection Systems by Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC http://www.securityfocusonline.com/

Intrusion Detection Systems; Definition, Need And Challenges. (2001). Retrieved March 7, 2015, from http://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343

Rouse, M. (2007, May 10). What is intrusion detection (ID)? - Definition from WhatIs.com. Retrieved March 7, 2015, from http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection

Intrusion Detection System - IDS Technology and Deployment. (n.d.). Retrieved March 12, 2015, from https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-detection-system-ids.html

*Beign, B., & Peer, P. (2012). Intrusion Detection and Prevention System: Classification and Quick Review. *ARPN Journal of Science and Technology, 2*(7), 661-661. Retrieved March 12, 2015, from http://www.ejournalofscience.org/archive/vol2no7/vol2no7_17.pdf

*Jaiganesh, V., Mangayarkarasi, S., & Sumathi, D. (2013). Intrusion Detection Systems: A Survey and Analysis of Classification Techniques. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(4), 1629- 1629. Retrieved March 13, 2015, from http://www.ijarcce.com/upload/2013/april/1-mangai amar-Intrusion Detection Systems.pdf