Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding Intrusion Detection Systems

The paper is designed to outline the necessity of the implementation of Intrusion Detection systems in the enterprise environment. The purpose of the paper is to clarify the steps that need to be taken in order to efficiently implement your Intrusion Detection System, and to describe the necessary components. The work should also clarify what you can expect of your Intrusion Detection System, and what you have to anticipate for, prior to deployment.

Copyright SANS Institute
Author Retains Full Rights

AD

Understanding Intrusion Detection Systems

1. Introduction

The paper is designed to outline the necessity of the implementation of Intrusion Detection systems in the enterprise environment. The purpose of the paper is to clarify the steps that needs to be taken in order to efficiently implement your Intrusion Detection System, and to describe the necessary components. The work should also clarify what you can expect of your Intrusion Detection System, and what you have to anticipate for, prior to deployment. Lets get started

2. Problem

Information Systems and Networks are subject to electronic attacks. Attempts to breach information security are rising every day, along with the availability of the Vulnerability Assessment tools that are widely available on the Internet, for free, as well as for a commercial use. Tools such as SubSeven, BackOrifce, Nmap, L0ftCrack, can all be used to scan, identify, probe, and penetrate your systems. Firewalls are put in place to prevent unauthorized access to the Enterprise Networks. Lets, however, ask ourselves: Are the firewalls enough?

During the course of 5 years, working as an Information Security officer, I found, that it is much easier even for the technically experienced professional to comprehend material, when you draw a real life picture of what might happen if the appropriate preventive work would not have taken place. So in the next paragraph I will attempt to show you such an example.

Imagine that you have just purchased a state of the art Home Theatre System. Everyone who knows anything about electronics, have an idea of how much it may cost. After installing it, you decided that you might need to install new locks on all the doors in your house, because the old ones do not use the up to date secure mechanisms. You call the locksmith, and in about 2 month (if you are lucky) you have a new locks on your doors, and you are the only one who have the keys (well, may be you mother have another pair). With that in mind you pack your things, and with whatever money you got left from you recent purchases, you go on vacation. As you came back a week later, you find that the Entertainment room looks different. After careful examination, you realize that your Home Theater System, that you were dwelling over for the last year, is missing. What worse is that your wife told you that the window in the kitchen is broken, and there is boot stains on the carpet, all over the house. That led you to believe that some one broke into your house, stole, and vandalized a lot of your prized possessions. After you wipe the tears from your eyes, you suddenly begin to vaguely remember the brochure that you got, about a burglar alarm installation in your neighborhood. You threw it away just a week before. The installation and monitoring would have cost you 19.95 a month with this promotional offer. Neglecting to install the system, is a secret that you would have to leave with for the rest of your life (your wife's engagement diamond ring was stolen as

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

well). Could you have prevented it from happening, were you to install an alarm? May be not completely, but the damage would be much less.

The real life example above is the exact same analogy of what might happen to your network. What's worth is that the thief may be on your network for a long time, and you might not even know it. Firewalls are doing a good job guarding your front doors, but they do not have a possibility to alert you in case there is a backdoor or a hole in the infrastructure. Script kiddies are constantly scanning the Internet for known bugs in the system, including constant scans by subnets. More experienced crackers may be hired by your competitors, to target your network specifically, in order to gain competitive advantage. The list of threats can go on.

3. What is the Intrusion Detection?

Intrusion Detection Systems help information systems prepare for, and deal with attacks. They accomplish this by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems.

Intrusion detection provides the following:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

There are three main components to the Intrusion detection system

- Network Intrusion Detection system (NIDS) – performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be send to the administrator. Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into your firewall
- Network Node Intrusion detection system (NNIDS) – performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device
- Host Intrusion Detection System (HIDS) – takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines, that are not expected to change their configuration

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4. What Intrusion Detection System CAN and CAN NOT provide

The IDS however is not an answer to all your Security related problems. You have to know what you CAN, and CAN NOT expect of your IDS. In the following subsections I will try to show a few examples of what an Intrusion Detection Systems are capable of, but each network environment varies and each system needs to be tailored to meet your enterprise environment needs.

The IDS CAN provide the following:

- CAN add a greater degree of integrity to the rest of you infrastructure
- CAN trace user activity from point of entry to point of impact
- CAN recognize and report alterations to data
- CAN automate a task of monitoring the Internet searching for the latest attacks
- CAN detect when your system is under attack
- CAN detect errors in your system configuration
- CAN guide system administrator in the vital step of establishing a policy for your computing assets
- CAN make the security management of your system possible by non-expert staff

The IDS CAN NOT provide:

- CAN NOT compensate for a weak identification and authentication mechanisms
- CAN NOT conduct investigations of attacks without human intervention
- CAN NOT compensate for weaknesses in network protocols
- CAN NOT compensate for problems in the quality or integrity of information the system provides
- CAN NOT analyze all the traffic on a busy network
- CAN NOT always deal with problems involving packet-level attacks
- CAN NOT deal with some of the modern network hardware and features

5. Where do I put my IDS?

Although these questions are largely dependent on your environment, we will try to identify the most common places that intrusion detection mechanisms are installed on. Please look at the following illustration taken from http://www.iss.net, and try to imagine your own environment and where would you place the sensors.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

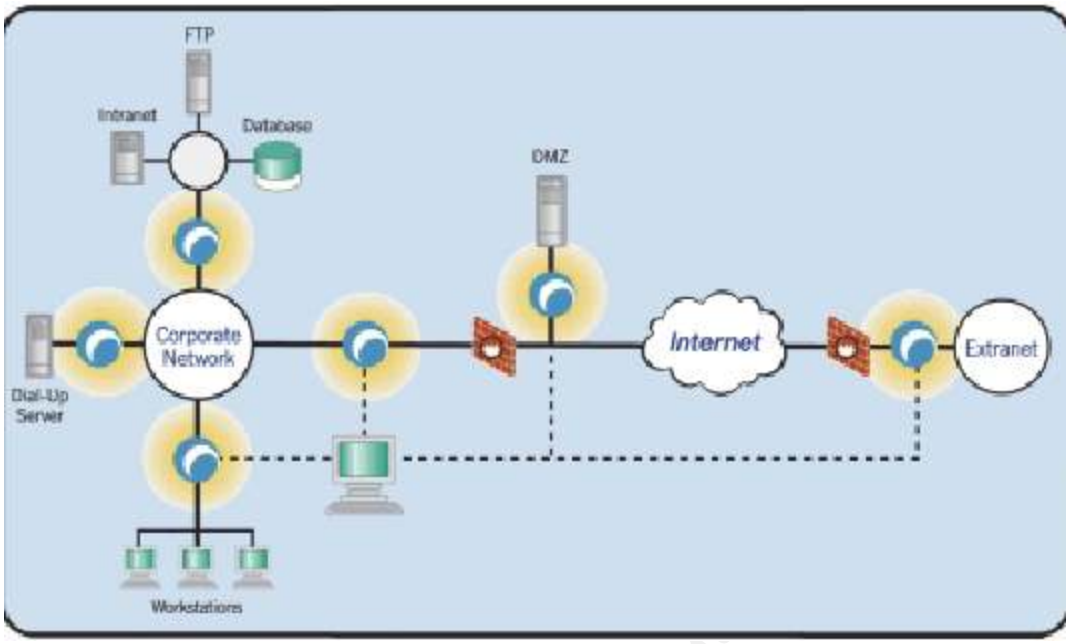

Figure 1.1 Sensors are represented by round blue dots

As you can see on a figure 1.1 the logical places for the sensors are:

- Between your network and Extranet
- In the DMZ before the Firewall to identify the attacks on your servers in DMZ
- Between the firewall and your network, to identify a threat in case of the firewall penetration
- In the Remote access environment
- If possible between your servers and user community, to identify the attacks from the inside
- On the intranet, ftp, and database environment

The idea is to establish your network perimeter and to identify all possible points of entry to your network. Once found IDS sensors can be put in place and must be configured to l report to a central management console. The dedicated administrators would logon to the console and manage the sensors, providing it with a new-updated signature, and reviewing logs. Remember to ask the vendor if the communication between your sensors and management console is secure. You do not want someone to temper the data.

6. **Who needs to be involved?**

In order to identify mission critical systems the following people MUST be involved:

- Information Security Officers

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Network Administrators
- Database Administrators
- Senior Management
- Operating System Administrators
- Data owners

Without those individuals involved, the resources will not be used efficiently. Vulnerably and risk assessment must be done prior to implementing IDS

7. My IDS is up, what now?

Once your IDS is up and operational, you must dedicate a person to administer it. Logs must be reviewed, and traffic must be tailored to meet the specific needs of your company. What may look abnormal to your IDS may be perfectly suitable for your environment. You must know that IDS must be maintained and configured. If you feel that you lack knowledgeable staff, get a consultant to help, and train your personnel. Otherwise you will loose a lot of time and money trying to figure out, what is wrong.

Emergency response procedure must exist and comply with your security Policy.

Emergency response procedure must outline:

- Who will be the first point of contact
- List all of the people who will need to be contacted
- Person responsible for decision making on how to proceed in the emergency situation
- Person responsible for investigation of the incident
- Who will handle media, in case the incident gets out
- How will the information about the incident will be handled

8. Where do I find an Intrusion Detection mechanism?

After we decided that we need an intrusion detection mechanism, we have to find out where do we get it. Bellow I provide a list of vendors that offer Intrusion Detection products and services. Products vary from freeware to commercially available

Freeware:

Snort - http://www.snort.org/
Shadow

Commercially Available:

RealSecure from ISS - http://www.iss.net/customer_care/resource_center/product_lit/
NetProwler from Symantec -
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50&PID=5863267
NFR - http://www.nfr.com/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

9. Conclusion

Hopefully this paper convinced you that IDS is a necessary tool in any environment, and you will take your time to try to persuade your management to implement it. Please remember that deploying IDS requires a lot of research and planing. Once configured correctly it will give you a world of benefit, but if you will neglect to properly configure it, IDS will give you a HUGE headache. Remember that security is not a Patch, which you can implement and forget about. It is a constantly changing concept that if not cared for will lead to disastrous results. Keep yourself constantly updated on the new events. Join web groups, read the news, sign up for alert notifications. If you are a Security Administrator for your company, you can not afford to be left behind, because it will usually mean failure. And failure will usually mean looking for a new job. Then you will never be able to afford that Home Theatre System you always wanted.

Hope you will find this papers helpful. Thank you

For more information please contact Danny Rozenblum at 201-206-6848 or dannyroz@yahoo.com

10. Cited Resources

1) Introduction to Intrusion Detection – ISCA Publications, Prepared by Rebeka Bace - URL: http://www.icsa.net/html/communities/ids/White%20paper/Intrusion1.pdf

2) Intrusion Detection and Response - Lawrence Livermore National Laboratory Sandia National Laboratories, December, 1996
URL: http://all.net/journal/ntb/ids.html

3) Intrusion Detection FAQ , SANS Institute
http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

4) GAO EXECUTIVE REPORT - B-266140
http://www.infowar.com/civil_de/gaosum.html-ssi

5) http://www.gocsi.com/intrusion.htm

6)Protection and Defense of Intrusion , Dorothy E. Denning Georgetown University March 5, 1996

http://www.cosc.georgetown.edu/~denning/infosec/USAFA.html

7) http://www.iss.net/securing_e-business/security_products/intrusion_detection/index.php

8) http://www.cerias.purdue.edu/coast/intrusion-detection/ids.html

9) http://www.nswc.navy.mil/ISSEC/CID/co-ordinated_analysis.txt

10) http://securityportal.com/articles/idssubjects20010226.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**