Global Information Assurance Certification Paper

An introduction to Intrusion Detection Systems

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1
Research on Topics
in Information Security

Submitted by : Philippe Bunel , December 09, 2004
Location : SANS Conference - LONDON June, 2004.

Table of Contents

List of Figures

Abstract

In the context where exchanges between Information Systems are important and it is more and more difficult to maintain efficiently and safely these systems, it is essential to ensure that people cannot realize malicious actions. Intrusion detection allows to keep it under control.

This document is an introduction to Intrusion Detection Systems(IDS). It will begin with a discussion about different types of detection mechanisms, then we will detail the possible responses to an attack, and different types of IDS. Finally it will mention the new concept of IPS (Intrusion Prevention System), and a discussion of possible ways to improve existing systems.

Introduction

Due to the fact that the Internet and local networks have become omnipresent, the number of intrusion events has grown. A security policy around these systems is essential. Its objective is to reduce the risks relating to: confidentiality, integrity, availability, and non-repudiation.

Organizations are gradually implementing systems that monitor IT security.

Since some years, companies have put in place several mechanisms in place to deal with computer system intrusions like; firewalls are used to filter inbound network traffics, Antivirus used to stop propagation of worm, authentication in order to control access data and VPN technology, to encrypt dataflow between headquarters and agencies over the Internet.

Unfortunately, these mechanisms have limitations; information systems have configuration breaches that allow the attackers to bypass security mechanisms.

A 2004 study from CSI/FBI[1] indicates that 98% of companies have firewall control products, 53% experienced an intrusion in the last 12 months[2].
Some systems protect from outside attacks, while several studies have revealed that near 70% of attacks were initiated from the inside.

A firewall enforces which traffic is allowed in and out a network, based on rules that have been defined. The firewall inspects the headers but not the contents of data packets. Many exploits attempt to take advantage of weaknesses in protocols that are allowed through the perimeter firewalls. Hackers will use your web server which has been compromised as a springboard to launch attacks on other internal servers.

That is why a second line of defence is necessary, the intrusion detection system (IDS). IDS have since a few years gained a considerable amount of interest, and they are an important component of defensive measures protecting computer systems and network from Abuse. However, that does not exempt organization to have a well defined and applied security policy, before implementing IDS.

A report from research group Gartner Inc has sparked off fierce debate in the intrusion detection system market. In the information Security Hype Cycle, R.

[1] CSI/FBI, Computer crime and security survey 2004, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[2] The percentage of organizations reporting computer intrusions decline since 5 years. It has been cited that the main raison, intrusions were not reported, is the negative publicity concern.

Stiennon[3] concluded that IDSs has failed to offer up any value to companies relative to their associated costs, and will be obsolete by 2005. He considers that IDS functionalities are moving into firewalls, which perform deep packet inspection. Some analysts do not agree with this affirmation.

The world of Intrusion Detection evolves rapidly; all commercial talks speak highly about IPS.

[3] R.Stiennon, Security Hype Cycle , Gartner Inc, www.gartner.com/5_about/press_realeases/pr11june2003c.jsp

Classification of Intrusion Detection Systems

Intrusion Detection is the art of detecting inappropriate or suspicious activity against computer or networks systems. Today, it is difficult to maintain computer systems or networks devices up to date, numerous breaches are published each day. IDS monitor the usage of such systems and detect the apparition of insecure states. This insecure state can be either an attempt from internal users to abuse their privileges or outside users (attackers) to exploit security vulnerabilities.

Anderson[4] introduced the concept of intrusion detection in 1980. He has been the first showing the importance of security audit trails in the aim of detecting policy violation. He defined a violation of policy security as a deliberate unauthorized attempt to:

- access information
- manipulate information
- make a system unreliable or unusable

Debar, Dacier, Wespi[5] have described an intrusion-detection system as a detector that processes information coming from system that is to be protected. This detector uses three kinds of information:

- technique used to detect intrusion (for example signature database),
- configuration information about the current state of system,
- audit trail

The detector eliminates all unnecessary information, determines if this action can be considered as a symptom of an intrusion, and takes an action (send alerts for example).

[4] J.P. Anderson, "Computer security threat monitoring and surveillance" April 15,1980 : http://csrc.nist.gov/publications/history/#ande80

[5] H.Debar, M.Dacier, A.Wespi "Towards a taxonomy of Intrusion-Detection Systems URL: http://perso.rd.francetelecom.fr/debar/papers/DebDacWes99.pdf

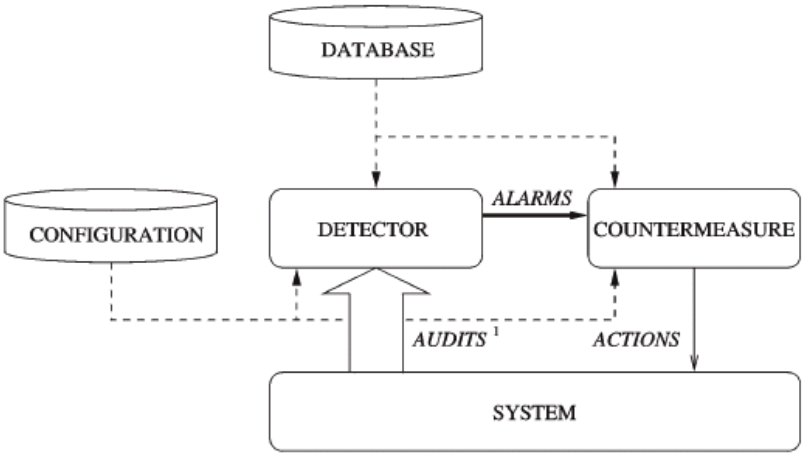

Figure 1- Simple Intrusion detection system[6]

They have also classified IDS according to some criteria:

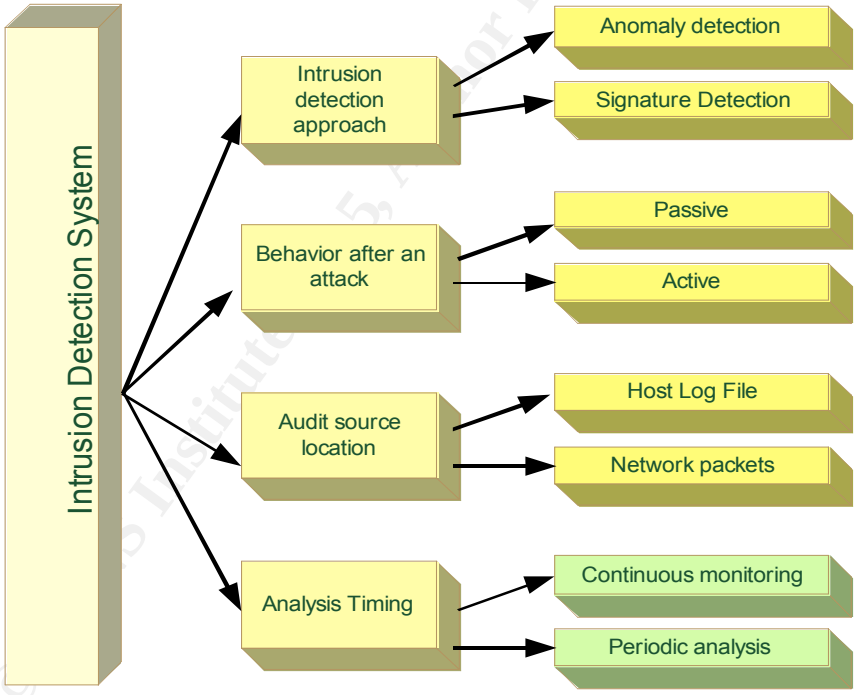

Figure 2- Characteristics of Intrusion Detection System [6]

The different characteristics will be detailed in the continuation of this document.

[6] H.Debar, M.Dacier, A.Wespi "Towards a taxonomy of Intrusion-Detection Systems URL: http://perso.rd.francetelecom.fr/debar/papers/DebDacWes99.pdf

Intrusion Detection approach

The most common approaches to Intrusion Detection are statistical anomaly detection and Misuse detection.

Anomaly Detection

Anderson[7] has proposed to describe statistically the usual user behavior, in order to detect all unusual actions of this user (specific hours of logon, system activity).

The study of anomaly detection was prefaced by the assumption that it would be possible to distinguish between a usurper and a legitimate user by identifying deviation from historical system usage.

It was hoped that an audit analysis approach would be useful to identify not only crackers who had acquired identification and authentication information to allow masquerading as legitimate users, but also legitimate users who were performing unauthorized actions.

This trend is referred to as “behavior based”; it consists in searching for evidence of attacks based on knowledge accumulated. Abnormally high CPU load combined with other metrics can indicate an intrusion in progress.

This model has the advantage of detecting new types of attacks; however, frequently adjustments are necessary to upgrade the reference model in order to reflect the normal user’s behavior and reduce among of false positive.

The majority of IDS based on Anomaly Detection are still under research projects. Some of these are: EMERALD[8], GrIDS[9], AAFID[10].

[7] J.P. Anderson, “Computer security threat monitoring and surveillance” April 15,1980 : http://csrc.nist.gov/publications/history/#ande80
[8] EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) http://www.sdl.sri.com/programs/intrusion/
[9] GrIDS (Graph Based Intrusion Detection System) http://www.cs.ucdavis.edu/research/tech-reports/1999/CSE-99-2.pdf
[10] AAFID (Autonomous Agents For Intrusion Detection) http://www.cerias.purdue.edu/about/history/coast/projects/aafid.php

Misuse Detection or Signature Detection

Another trend consists to model prohibit behavior. This trend is often referred to "Misuse detection" or "Signature Detection". It is based on the search for evidence of attacks based on the incremental knowledge from known attacks. This type of IDS can only detect attacks which it has the signature. Frequently updates are necessary to maintain up to date the knowledge database.

The efficiency of this trend depends on the precision of the signatures. That is why this system can be bypassed by attackers who use evasion techniques, to make their attacks undetectable. An exploit code can often easily change (polymorphic buffer overflow for example), and this attack will not be detected. Enough techniques exist to get around IDS, you can refer to the K.Timm's document[11] for more details in this subject.

It is possible to create generic signatures that can detect more variants of the same attack, but it is necessary to have a good understanding of attacks, and network components in order to block malicious activities, and not deny valid traffic.

A signature defines the characteristics of an attack (protocol, service, source, pattern) you can see an example with a snort signature; this event is generated when an attacker attempts to retrieve /etc/password file into a web server.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-
MISC /etc/passwd"; flow:to_server,established;
content:"/etc/passwd"; nocase; classtype:attempted-recon; sid:1122;
rev:5;)
```

Figure 3 - Snort signature[12]

These two approaches can lead to generate *"False positive"* and "*False Negative"*:

- A tool based on Anomaly Detection approach will generate an alert if it detects an unknown behavior. If this deviation is due to the normal system evolution, this alert is a false positive; on the other hand, an attacker can modify gradually his behavior to reach an intrusive behavior. If this intruder realizes an exploit, and this exploit is not detected, it is a false negative.

- A tool based on "Misuse detection" is less impacted by false positive because all abnormal activities are described in signature database. However, if a pattern

[11] Kevin Timm, IDS Evasion Techniques and Tactics May 7, 2002, http://www.securityfocus.com/infocus/1577
[12] Snort Signature Database, http://www.snort.org/snort-db/sid.html?sid=489

matching quality is too bad, it can be lead to generate many of false positive. In case of a new attack, the signature database may not contain the signature; therefore the attack will not be detected.

Denning [13] has worked in the middle of 80's to merge these two approaches, and they have produced the first Hybrid IDS name IDES (Intrusion Detection Expert System). That system was enhanced to form NIDES[14], the Next-Generation Intrusion Detection Expert System. Despite of the fact that this has been improved, the Anomaly detection approach has been progressively given up in favor of "Misuse detection".

Today, Misuse-based detection is the most prevalent form of available IDS on the market.

Intrusion Responses

The type of the behavior after an attack depends on the IDS used. The passive response is available for all IDS, the active response is not very widespread.

Passive response: consist to register detected intrusions in a log file which will be analyzed by the security administrator. That does not prevent an attack to occur.

Active response: The aim is to stop an attack at the moment which occurs.

For this, two techniques exist, the firewall rules reconfiguration (which depends on firewall) and interrupt TCP connection.
The reconfiguration of firewall allows to block the malicious traffic by closing the offending port or to forbid the attacker's address.
The second technique stops the established session between an attacker and his target in order to stop data transfer or data modification on the target server.
For this, IDS send TCP reset packet on this two servers. Both servers think that the other was disconnected.
In case of active response, we must ensure that the malicious traffic is effectively a malicious one, otherwise legitimate users can be disconnected.
Generally, active response is used on a little among of certified alarms; Passive response is used for all others. For a complete view of all attacks, alerts files must be analyzed.

Types of IDS

There are mainly two types of Intrusion Detection Systems:

[13] Dorothy E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, February 1987. URL: http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf
[14] NIDES, http://www.sdl.sri.com/projects/nides/whatisnides.html

HOST-Based IDS (HIDS)

Host-based systems were the first type of IDS being developed and implemented. (SMF file on mainframe environment).It differs from network-based intrusion detection the entire process is conducted on the host itself.

These systems are deployed locally on each host computer and monitor only the host on which it is installed. They are typically placed on business critical hosts and on servers in a DMZ that are likely to be compromised.

The HIDS operates by monitoring changes to a number of variables on the host system. These controls may include: System processes, registry entries, CPU Usage, file access and integrity checking, audit policies, user accounts, events logs.

Exceeding the threshold or suspicious integrity changes will send an alert to administrators. HIDS can help to detect abnormal behavior on a computer that might have been compromised, but an administrator system must spend enough time to analyze the HIDS output regularly, and suppress all false positive alerts.

HIDS Implementation

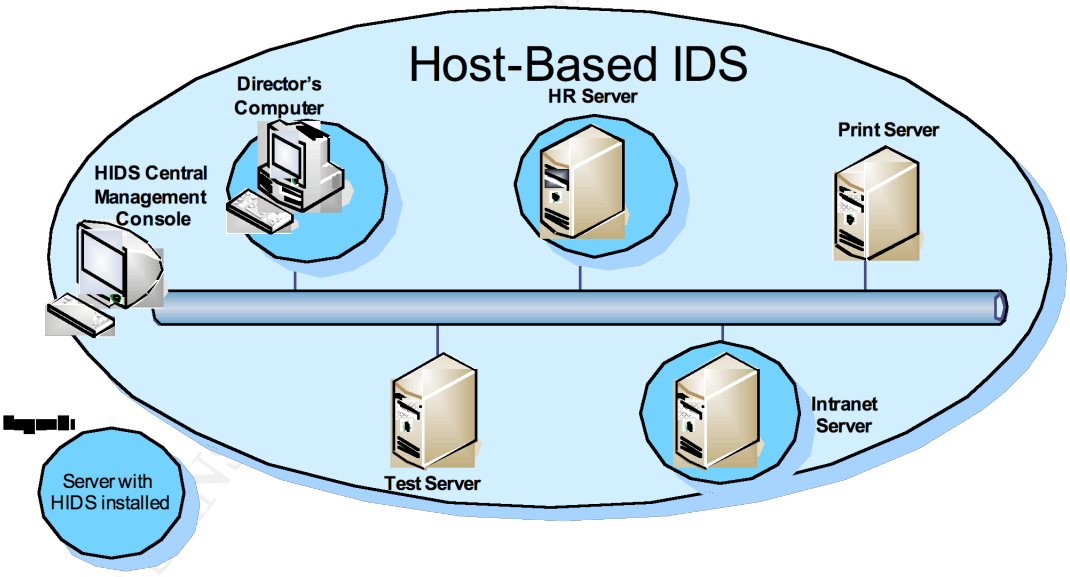

Figure 4 – Host-Based Intrusion Detection

Some HIDS tools: Symantec Host IDS[15], ISS BlackICE PC[16], TCPWrappers[17], Enterasys Dragon Host Sensor[18].

[15] SYMANTEC, Symantec Host IDS, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48
[16] ISS BlackICE PC Protection, http://www.digitalriver.com/dr/v2/ec_MAIN.Entry10?V1=253470&PN=1&SP=10023&xid=26412&CID=0&DSP=&CUR=840&PGRP=0&CACHE_ID=0

Integrity Checkers

Some analyst consider Integrity checkers as part of HIDS, and think that vendors will integrate them soon in their HIDS solutions.
If a method of attack is unknown, then only indirect evidence of its presence (effects) can be detected. Then integrity checkers can help to detect intrusions. When attackers make change in systems; they often create backdoors, or delete logs to hide evidence of their activity. Attackers may be able to evade signature-based IDS, but it's more difficult to escape from the notice of integrity checker tools.

Tripwire is an example of integrity tool[19].

Network-Based IDS (NIDS)

The NIDS are probably the most known systems. They are installed on a network and act like a sniffer (stealth mode or promiscuous mode), capturing and decoding packets to pass through his network segment. This probe analyzes IP packets with the aim to locate signature attacks. Unlike HIDS, NIDS can monitor an entire network segment and can be rapidly deployed.

Although a NIDS is a valuable tool, it has major limitations for processing traffic:

- In switched network: NIDS presents an issue on a switched network. By designing a switch functions which only transmit packets directly to the intended recipient of packet and not the entire network like a conventional hub based networks. To solve this point, we can use the spanning port (used generally for debugging purpose) or a network tap. This port receives all traffic transmitted on the switch.

- On high speed networks: Speed is a serious factor to consider when deploying IDS solution because underpowered IDS will not be able to capture all the traffic when his limit is exceeded. Furthermore, an attacker can flood your network in order to perform an exploit, and this exploit will not detect. Vendors have created Appliance solutions (dedicated hardware) to improve performance.

- Encrypted networks: If an attacker uses SSH to connect to a machine, the NIDS cannot send an alert because the traffic is encrypted. In this case, HIDS can be used to determine the behavior evolution on this machine.

[17] TCPWrappers, ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
[18] Enterasys Dragon Host Sensor, http://www.enterasys.com/products/ids/
[19] Tripwire, Commercial version: www.tripwire.com General Public License: www.tripwire.org

NIDS Implementation

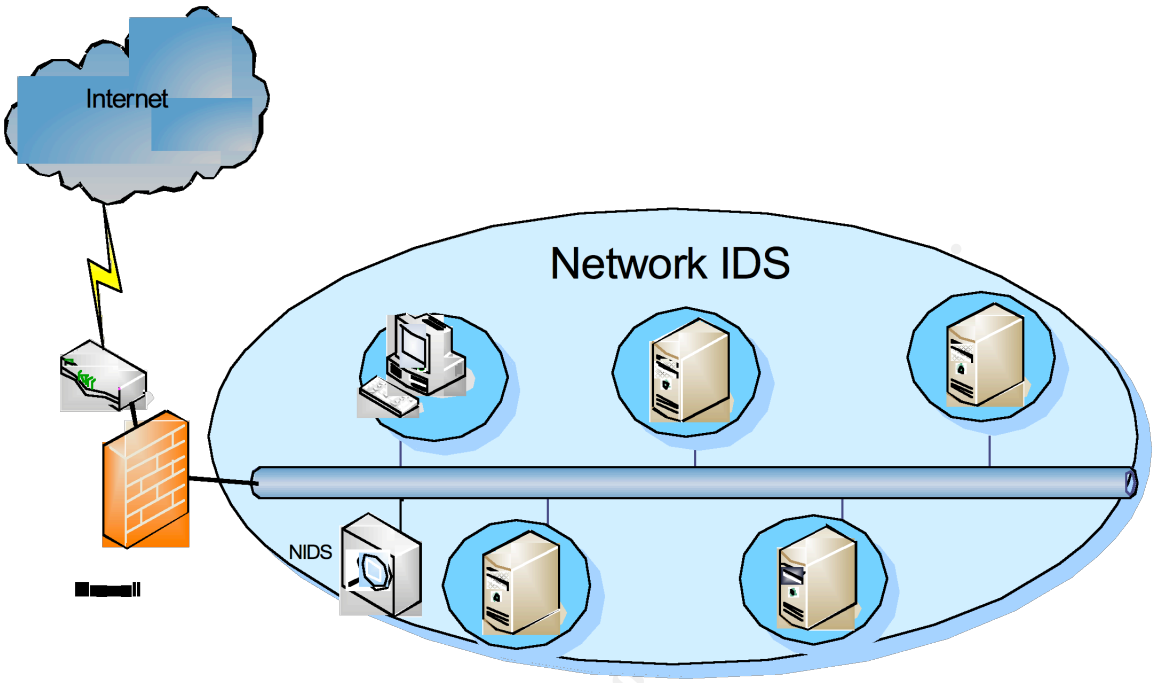

Figure 5- Network-Based Intrusion Detection System

Since HIDS, and NIDS are complementary, some IDS vendors propose three tiered architecture that integrate both HIDS and NIDS sensors, and a central Management console. The security team can remotely access this centralized server to analyze the logs, run reports, manage the configurations of the sensors, and customize the intrusion detection policy.

Here's some example of NIDS: Cisco NetRanger[20], NFR[21], Dragon[22], Snort[23], ISS Realsecure[24].

IDS Evolution

IPS versus IDS

Anyone who works regularly with IDS has probably been overwhelmed by a large amount of false positive. That is why most of current IDS have doomed to disappear or evolve extremely. The apparition on the market of IPS (Intrusion

[20] Cisco NetRanger, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/
[21] NFR security, http://www.nfr.com/solutions/sentivist-ids.php
[22] Dragon, http://www.enterasys.com/products/ids/dragon7-overview.pdf
[23] Snort, http://www.snort.org/
[24] ISS Realsecure, http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php

Prevention System) is recent and it involves improving the solutions. IPS objective is to anticipate hacker's attacks as soon as a "footprint" is known. He must not only react to an attack in progress, but also prevent that this one begins. An IPS is put inline and examines all in/out packets, and can affect the speed of the network (bottleneck) if it is underpowered.

An IPS must also be able to:
- understand IP networks (existing architecture, protocol used, applicative layer in order to detect protocol anomalies
- work in "statefull inspection" mode in order to known at each instant the context of the current analyze.

Some example of IPS: Arkoon IPS[25], ISS Proventia G series[26]. Some firewalls have IPS integrated, like Netasq IPS-Firewall[27] for example.

One of IPS problems is that they can only detect the act of infection, whereas companies would like also to detect the result of the infection. To do this the following solution is available: continuous scanning; active scanning is an intrusive technology that can induce software instabilities in the scanned servers, and use network bandwidth. Between two active scans, a port can appear and disappear, security administrator will not be informed that a backdoor exists in his payroll server. An alternative method exists: passive scanner.

Passive vulnerability scanner

Passive vulnerability scanning is the process of monitoring network traffic at the packet layer; discover operating system, list of open port and application information. Unlike active scanner, this is a non-intrusive method which operates 24x7 without human intervention. It 'sniffs' the traffic much like a network IDS or protocol analyzer. In order to accomplish this, it must be deployed, like a conventional NIDS, on a network hub, spanned port of a switch or on a network tap. However, passive network monitoring is dependent on the traffic. Without traffic, no vulnerabilities will be detected and no alert sent.

Two products are under this category: Sourcefire RNA sensor[28], Tenable Nevo[29].

Other innovative techniques can be used to reduce the problem of false positives and have a best knowledge of attacks.

[25] Arkoon IPS, http://www.arkoon.net/EN/
[26] ISS Proventia, http://www.iss.net/products_services/enterprise_protection/proventia/g_series.php
[27] NetASQ IPS-Firewall, http://www.netasq.com/
[28] SourceFire RNA sensor, http://www.sourcefire.com/products/rna.html
[29] Nevo, Tenable Security, http://www.tenablesecurity.com/products/nevo.shtml

Honeypots

Honeypot is a system used to simulate one or more network services that you designate on your computer's ports. An attacker assumes you are running vulnerable services that can be used to break into the machine. It can be used to log access attempts to those ports including the attacker's keystrokes. Honeypots can provide early warning about new attack and exploitation trends and they allow in-depth examination of adversaries during and after exploitation of the honeypot. There are no reason for legitimate traffic to access this resource, so any attempt to connect can be considered like an attack. We can use these data to correctly tune our system defence and mitigate a large part of attacks. Some IPS product like “Juniper Networks NetScreen-IDP”[30] use honeypots.

IDS Cooperation

As we can see, each IDS approach has its strengths and weaknesses. It will be interesting to correlate alarms, in order to reduce the rate of false positive and have a global vision of security state on Information System. A numerous IDS (commercial or free) are available on the market; some of these are aimed at detecting intrusions on the network, others on hosts, and a minor category, applications. Currently, there is no normalisation of exchange message format between different vendors. Solutions that exist depend on vendors.

The Intrusion Detection Exchange Format Working Group (IDWG) has written a document “Intrusion Detection Message Exchange Format (IDMEF)”[31]. IDMEF is planned to be a standard format which automated IDS can use for reporting what they have deemed to be suspicious.

Human Factor

Human factor plays a preponderant role in the solution of IDS implementation. Putting up a ‘box’ is not enough. A suitable solution must be found and used. A long study is necessary before putting into production. Then logs will be analyzed by team which must show its ability to understand (security skills are needed) and take appropriate measures as upgrading the knowledge base, for instance.

[30] Juniper Networks NetScreen-IDP , http://www.juniper.net/products/intrusion/dsheet/110010.pdf
[31] The Intrusion Detection Message Exchange Format draft-ietf-idwg-idmef-xml-12.txt, http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-12.txt

Summary

Security incidents are growing up every day, therefore implementing an effective IDS appears to be more and more necessary. IDS must be integrated with all the other security tools implemented within the I/T infrastructure.

Deploying a combination of host-based and network-based detection systems in critical systems can be a good choice. On the other hand, we keep in mind the costs associated with such deployment; product cost, duration of installation and the workload needed to analyze logs sent by IDS into the console. Numerous false positive exist, that explains why new solutions appear, but they are still not reliable.

Nevertheless, these technologies are lead to be developed in the forthcoming years with the security need of companies and the evolution of technologies that allow a more efficient functioning of IDS/IPS.

However, vendors of security solutions integrate IDS/IPS directly in firewalls in order to improve the cooperation between these elements, the work of IDWG Group also go in this way. These systems will have a certain degree of autonomous response in order to reduce the administrator's workload.

Glossary

Intrusion Detection :
An ID gathers and analyzes information from various areas with a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Network IDS: (NIDS)
A network IDS system monitors the traffic on its network segment. This is generally accomplished by placing the network interface card in promiscuous mode to capture all traffic across its network segment.

Host IDS: (HIDS)
A HIDS is software that resides on a host machine. It monitors the inbound and outbound traffic, the integrity of specific files, log files. When the threshold is exceeding, or a suspicious integrity changes is made, it sends an alert.

False Positive:
A False Positive is when the IDS return an alert about network traffic that is not malicious.

False Negative:
A False Negative is when an IDS fails to alert when a valid attack occurs.

References

[1] CSI/FBI, Computer crime and security survey 2004, URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[3] R.Stiennon, Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure, Garner Press release, June 11, 2003, URL: www.gartner.com/5_about/press_realeases/pr11june2003c.jsp

[4][7] Anderson, James P., "Computer security threat monitoring and surveillance" April 15,1980 , Fort Washington, URL: http://csrc.nist.gov/publications/history/#ande80

[5][6] H.Debar, M.Dacier, A.Wespi "Towards a taxonomy of Intrusion-Detection Systems, URL: http://perso.rd.francetelecom.fr/debar/papers/DebDacWes99.pdf

[8] EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), URL: http://www.sdl.sri.com/programs/intrusion/

[9] GrIDS (Graph Based Intrusion Detection System) http://www.cs.ucdavis.edu/research/tech-reports/1999/CSE-99-2.pdf

[10] AAFID (Autonomous Agents For Intrusion Detection), URL: http://www.cerias.purdue.edu/about/history/coast/projects/aafid.php

[11] Kevin Timm, IDS Evasion Techniques and Tactics May 7, 2002, URL: http://www.securityfocus.com/infocus/1577

[12] Snort Signature Database, URL: http://www.snort.org/snort-db/sid.html?sid=489

[13] Dorothy E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering,* February 1987. URL: http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf

[14] NIDES, http://www.sdl.sri.com/projects/nides/whatisnides.html

[15] SYMANTEC, Symantec Host IDS, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48

[16] ISS, BlackICE PC Protection, http://www.digitalriver.com/dr/v2/ec_MAIN.Entry10?V1=253470&PN=1&SP=10023&xid=26412&CID=0&DSP=&CUR=840&PGRP=0&CACHE_ID=0

[17] TCPWrappers, ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz

[18] Enterasys, Dragon Host Sensor, http://www.enterasys.com/products/ids/

[19] Tripwire, Commercial version: www.tripwire.com General Public License (GPL) version : www.tripwire.org

[20] Cisco, NetRanger, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/

[21] NFR, security, http://www.nfr.com/solutions/sentivist-ids.php

[22] Enterasys, Dragon, http://www.enterasys.com/products/ids/dragon7-overview.pdf

[23] Snort, http://www.snort.org/

[24] ISS, Realsecure, http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php

[25] Arkoon IPS, http://www.arkoon.net/EN/

[26] ISS Proventia, http://www.iss.net/products_services/enterprise_protection/proventia/g_series.php

[27] NetASQ Frewall, http://www.netasq.com/

[28 SourceFire, RNA sensor, http://www.sourcefire.com/products/rna.html

[29 Tenable Security, NEVO, http://www.tenablesecurity.com/products/nevo.shtml

[30] Juniper Networks NetScreen-IDP , http://www.juniper.net/products/intrusion/dsheet/110010.pdf

[31] IETF-IDWG, The Intrusion Detection Message Exchange Format, draft-ietf-idwg-idmef-xml-12.txt, http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-12.txt

Note: All URL listings have been verified as being active as of December 8, 2004

Books

Track1 – Sans Security Essentials v2.2 – Internet Security Technologies – 2004