ISSN 2277-3061

DEVELOPMENT OF AN INTRUSION DETECTION SYSTEM IN A COMPUTER NETWORK

[1]Babatunde, R.S.,
ronke.babatunde@kwasu.edu.ng
[2]Adewole, K.S.,
adewole.kayode@unilorin.edu.ng
[1]Abdulsalam, S.O.,
sulaiman.abdulsalam@kwasu.edu.ng
[1]Isiaka, R.M.,
abdulrafiu.isiaka@kwasu.edu.ng
[1]Department of Computer, Library and Information Science,
Kwara State University, Malete, Nigeria
[2]Department of Computer Science,
University of Ilorin, Ilorin, Nigeria

ABSTRACT

The development of network technologies and application has promoted network attack both in number and severity. The last few years have seen a dramatic increase in the number of attacks, hence, intrusion detection has become the mainstream of information assurance. A computer network system should provide confidentiality, integrity and assurance against denial of service. While firewalls do provide some protection, they do not provide full protection. This is because not all access to the network occurs through the firewall. This is why firewalls need to be complemented by an intrusion detection system (IDS).An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than proactive agent. It plays the role of an informant rather than a police officer. In this research, an intrusion detection system that can be used to deny illegitimate access to some operations was developed. The IDS also controls the kind of operations performed by users (i.e. clients) on the network. However, unlike other methods, this requires no encryption or cryptographic processing on a per-packet basis. Instead, it scans the various messages sent on a network by the user. The system was developed using MicrosoftVisual Basic.

Indexing terms:

Intrusion detection system, illegitimate, misuse, network.

Academic Discipline

Computer Science

Subject Classification

Computer Science

Method/Approach

Experimental

INTRODUCTION

Intrusion detection systemshave become an important component in the world of Computer Network Security. However, many security experts are still in the dark about IDS, not certain about what IDS tools do, how to use them, or why they must employ them.Intrusion detection is the process of monitoring computers or networks from unauthorized entrance, activity, or file modification[1]. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack such as a denial of service attack.If there are attacks on a system, we would like to detect them as soon as possible (preferably in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does.It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data[3].

However, completely preventing breaches of security appear, at present, unrealistic. These intrusion attempts can be detected and proper action may be taken to repair the damage later. [2],while introducing the concept of intrusion detection, defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt toaccess information, manipulate information, or render a system unreliable or unusable. Since then, several techniques for detecting intrusions have been proposed in the literature. Intrusion detection systems do exactly as the name suggests. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. An IDS installed on a network provides much the same purpose as a burglar alarm system installed in a house[2].

Although IDSs may be used in conjunction with firewalls, which aim to regulate and control the flow of information into and out of a network, the two security tools should not be considered the same thing. Firewalls can be thought of as a fence or a security guard placed in front of a house[4]. They protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system. They do not fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety[7].

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected[6]. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, or email. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts[8].

The most popular way to detect intrusions has been by using the audit data generated by the operating system. An audit trail is a record of activities on a system that are logged to a file in chronologically sorted order. Since almost all activities are logged on a system, it is possible that a manual inspection of these logs would allow intrusions to be detected. However, the incredibly large sizes of audit data generated (on the order of 100 Megabytes a day) make manual analysis impossible. IDSs automate the drudgery of wading through the audit data jungle. Audit trails are particularly useful because they can be used to establish guilt of attackers, and they are often the only way to detect unauthorized but subversive user activity[5].

Many times, even after an attack has occurred, it is important to analyze the audit data so that the extent of damage can be determined, the tracking down of the attackers is facilitated, and steps may be taken to prevent such attacks in future. An IDS can also be used to analyze audit data for such insights[2]. This makes IDSs valuable as real-time as well as post-mortem analysis tools. An overview of intrusion detection systems including a description of what IDSs are, the functions they serve, the two primary types, and possible future directions of research on IDS were discussed in this paper.

2.0 LITERATURE REVIEW

IDS research has been an active area for quite a while so there are many papers that have taken many different approaches. The analysis of Intrusion Detection Systems literature history starts with a paper in 1980 by James Anderson [2]. Anderson's paper does not actually mention IDS in words but does provide the foundations for the concept in a network monitoring system he called "surveillance program" to monitor threats from inside and outside an organization. His 1980 paper was a follow on from the 1972 paper called Computer Security Technology Planning Study which is generally regarded as being a classic forerunner to many of today's concepts [2].

The first IDS were very limited in their functionality and flexibility. In the earlier days some IDS vendors did not allow users to write their own rules/signatures. Some vendors would not even allow their customers to view the rule list that came with the IDS. Under such circumstances customizing a rule set based on one's network is totally out of the question[1]. They would be overwhelmed b

with stateless filtering was that it allowed hackers who fragmented their attacks to go undetected. Fragmented traffic has been used to create Denial of Service (DOS) attacks on routers, firewalls, and workstations. Insertion and evasion attacks could easily bypass stateless IDS [14].

IDS of past also did not have the ability to decode the protocol to see if the signature of a rule was needed to be scanned or not. An example is if you do not use the FTP command "put" but, you build a signature to alert when the "put" command is found. Without protocol decoding anytime the letters "put" showed up in anything from an email to a document, the alert would go off thus creating false positives. With protocol decoders the IDS knows to only apply the rule for “put” when the protocol is FTP. IDS sensors in the past could not sustain high speed traffic volume thus they would drop packets when the traffic load was too large[16]. Large networks with multiple connections to the internet faced a major challenge of being able to correlate information that was gathered over multiple sensors to try to turn the information into a useful data. According to [15], it was difficult to detect slow stealth scans that would come through multiple sensors (especially if the analyst had to switch back and forth between screens looking at the alerts).

A new concept was introduced in 1990, with NSM (Network Security Monitor or Network Intrusion Detector -NID). Instead of examining the audit trails of a host computer system, suspicious behaviour was detected by passively monitoring the network traffic in an entire LAN segment [4].This helps company/organisation owners to be able to form a basis for strategic planning/decision and specific management level. In 1991, a different idea was introduced with NADIR (Network Anomaly Detection and Intrusion Reporter) which is a rules based expert system developed at Los Alamos to automatically detect intrusion attempts and other security anomalies (Jackson 1991). Specific rules help to bring down the percentage of false positives butthen require constant maintenance and upgrade as new threats occur.

The next stage in the progression of IDS was DIDS (Distributed Intrusion Detection System) where the audit data from multiple hosts is collected and aggregated in order to gather intelligence on wide ranging threats and give an overall picture of the state of the network [9]. The system developed in this project is a specialized DIDS. In 1994, Mark Crosbie and Gene Spafford suggested the use of autonomous agents in order to improve IDS. The idea being that these autonomous agents could cooperate and gather information together to make the detection of intrusion more efficient [8].

IDS systems that have evolved to monitor movement of intellectual property embodied in a document of some sort are a future development. This is especially useful for companies that have outsourced their facilities to another country and so wish to make extra precautions against loss of company data. A very recent exampleis by Fidelis of Washington DC [18].

Currently, some of the major issues of the past have been resolved. Users are allowed to write their own rules list to customize their own network even with commercial IDS such as NFR’s (Network Flight Recorder) IDS [19]. Users are able to specify filters with great detail today. Filters can be set on IP, port, source/destination, protocol, TCP flag combinations, and content strings. For faster IDS performance some IDS will allow the user to specify where to begin looking for a string or how far to look for the string. For example, searching for the content beginning at the 5th byte in the application payload and searching the next 15 bytes would end on byte 20 in the payload [24].

2.1 IDS TECHNIQUES

There are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring, and stealth probes [26].

2.1.1 Anomaly Detection

This is designed to uncover abnormal patterns of behavior.The IDS establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion. What is considered to be an anomaly can vary, but normally, any incident that occurs on frequency greater than or less than the standard deviations from the statistical norm raises an eyebrow. An example of this would be if a user logs on and off of a machine 20 times a day instead of the normal 1 or 2. Also, if a computer is used at 2:00 am when normally no one outside of business hours should have access, this should raise some suspicions. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators.

2.1.2 Misuse Detection or Signature Detection

Misuse Detection commonly called signature detection, is a method that uses specific known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures [22]. For host-based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet content signatures and/or header content signatures can indicate unauthorized actions, such as improper FTP initiation[15]. The occurrence of a signature might not signify an actual attempted unauthorized access (for example, it can be an honest mistake), but it is a good idea to take each alert seriously. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response, or notification should be sent to the proper authorities.

2.1.3 Target Monitoring

These systems do not actively search for anomalies or misuse, but instead looks for the modification of specified files. This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals [10]. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the system critical files.

2.1.4 Stealth Probes

This technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers, for example, will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks[14]. Stealth probes collect a wide-variety of data throughout the system, checking for any methodical attacks over a long period of time. They take a wide-area sampling and attempt to discover any correlating attacks. In effect, this method combines anomaly detection and misuse detection in an attempt to uncover suspicious activity.

2.2 TYPES OF INTRUDERS

The types of intruders according to (Akbar *et al.*, 2011)are:

i. **External Intruders**: These are unauthorized users who enter the system, make changes to the system and access the resource in the network without authorization.

ii. **Internal Intruders**: These are intruders in the network without user accounts trying to attack the system.

2.3 IDS CATEGORIES

The categories of IDS with respect to the location of intrusion are:

i. **Network Intrusion Detection System (NIDS)**: This is a network based IDS that monitors the network for mischievous traffic and individual packets information exchange.

ii. **Host Intrusion Detection System (HIDS)**: This monitors the activities such as system calls, application logs, and password files, what files were accessed, what applications were executed with a particular host.

3.0 EXPERIMENTAL SETUP

The developed Intrusion Detection System has four main components;

i. The central analysis server monitoring the network.

ii. The IDS.

iii. The database system of the IDS that is referenced.

iv. The Visual Basic application used to access the database.

3.1 The Central Analysis Server

The central analysis server is the heart of the operation. This server consists of a database and Web server to see the current attack status of the network. It also listens to the clients on the network and uses the misuse detection technique to check and verify the messages sent by users on each workstation connected to it.

3.2 The developed IDS

The technique adopted in this research for the development of the IDS is misuse detection. Some known words/signature that are mostly found in illegitimate mails (junk, spam) were gathered from some search engines and were used to design a database of attack signature. The IDS monitors the operation performed on the network and if any illegitimate operation (such as sending spam, junk or hacking messages and opening of illegal website) is detected, an alert is sent to the server, which automatically classifies the mail contents and send the outcome of classification to the client.

3.3 The database system of the IDS that is referenced

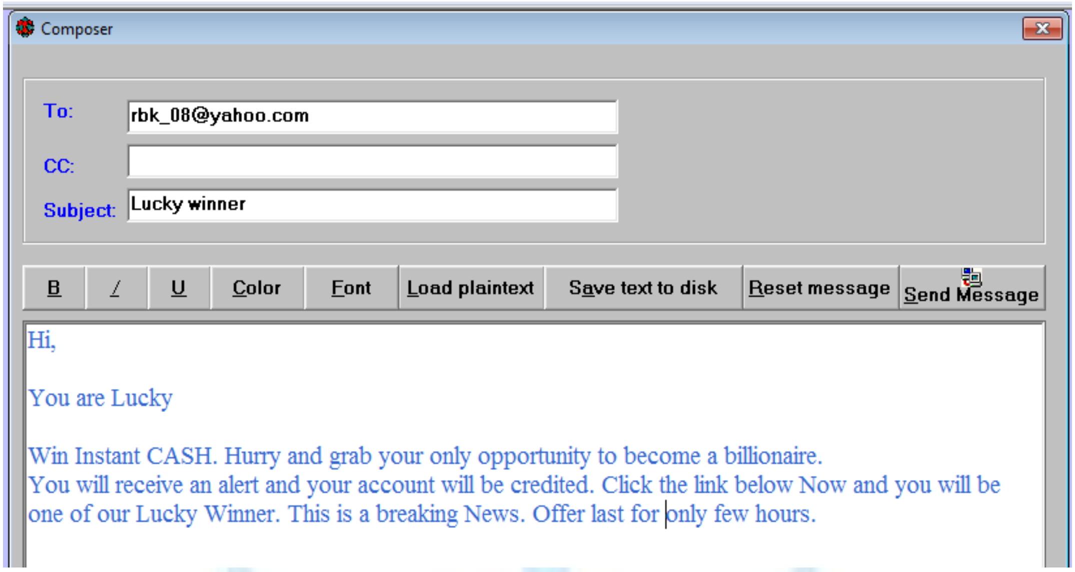
SQL server database management system was used to create and monitor the database of the proposed IDS software. The software was linked with the database using the technique of open database connectivity (ODBC) which makes it easy to connect several databases to a single application.

3.4 The Visual Basic application used to access the database

This application was developed in order to provide an interface for the user. This allows a user to access the database remotely.The ability of Visual Basic to keep variables private whilst accessing network resources on behalf of a user enhances security immensely. Also, the fact that the Visual Basic application would enable access to the IDS database without having to give command line access to the user increases security even more.

4. RESULTS AND DISCUSSION

The customized message composer is displayed in Figure 1 where users can compose messages to be sent. Once the user is done typing and clicks on send button, the server sends a response to alert the user, prompting the user that the mail content as classified by the IDS is malicious. If the user continues by clicking send button again, the message prompt in Figure 2 is displayed and the server shuts down the client's system automatically.



To: rbk_08@yahoo.com

CC:

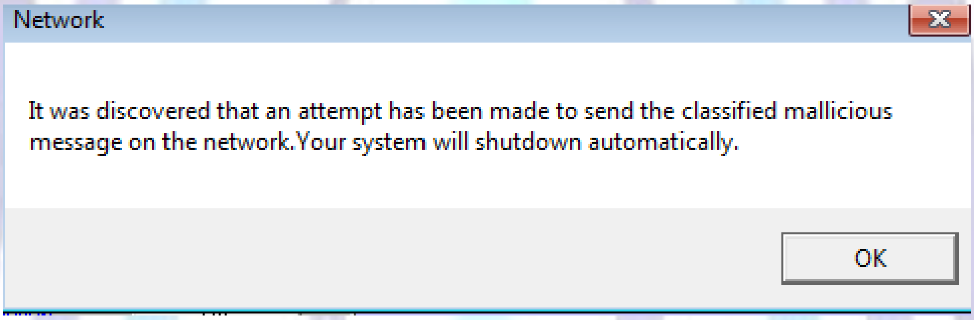
Subject: Lucky winner

Hi,

You are Lucky

Win Instant CASH. Hurry and grab your only opportunity to become a billionaire.
You will receive an alert and your account will be credited. Click the link below Now and you will be one of our Lucky Winner. This is a breaking News. Offer last for only few hours.

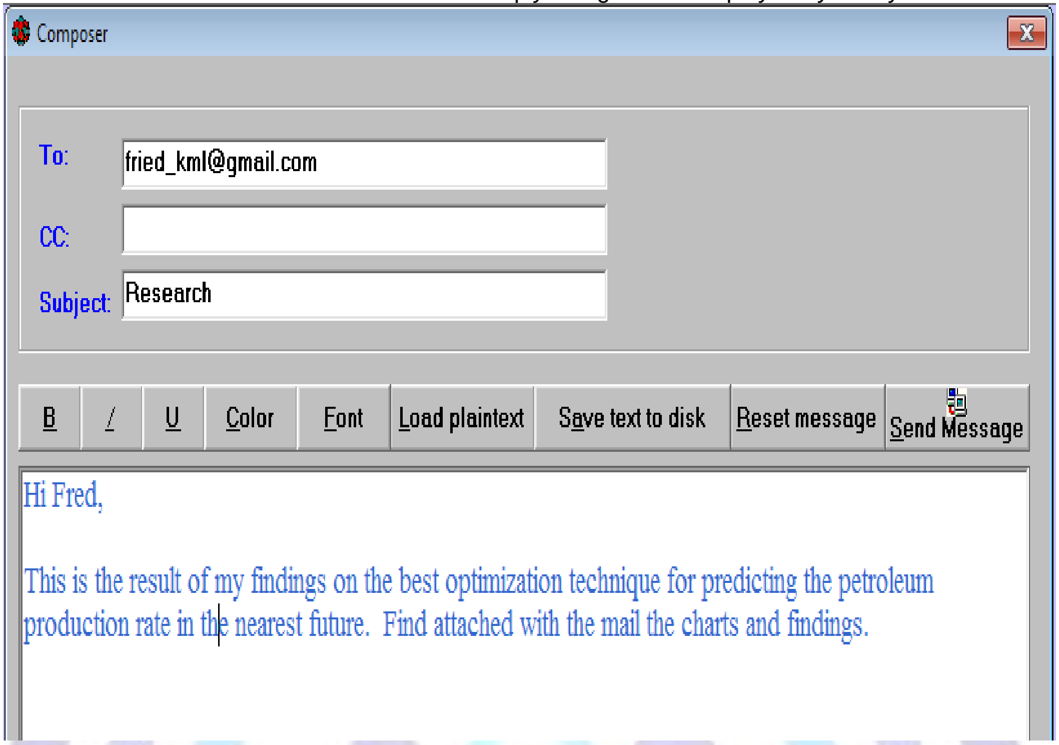
Figure 1: The Customized message composer- a malicious message



It was discovered that an attempt has been made to send the classified mallicious message on the network.Your system will shutdown automatically.

Figure 2: A message, warning the client that insists on sending junk mail.

However, if a user composes a message classified by the IDS as normal, such as the one shown in Figure 3, the message will be sent to its destination and the reply in Figure 4 is displayed by the system.



To: fried_kml@gmail.com

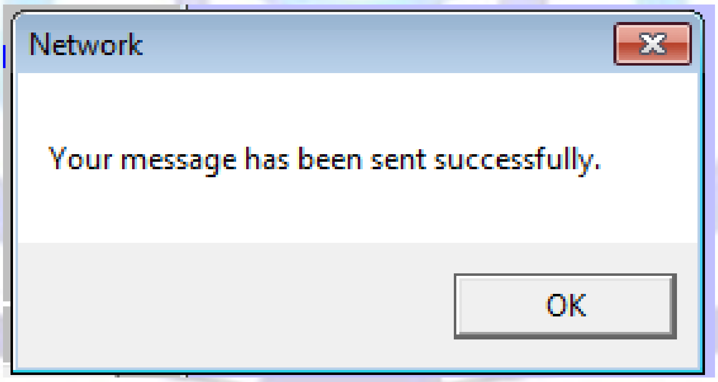
CC:

Subject: Research

Hi Fred,

This is the result of my findings on the best optimization technique for predicting the petroleum production rate in the nearest future. Find attached with the mail the charts and findings.

Figure 3: The Customized message composer- a normal message



Your message has been sent successfully.

Figure 4: Reply after sending normal message

5. CONCLUSION AND FUTURE WORK

In this paper, an IDS software is developed which monitors users activities on a network and categorizes various operations using misuse/signature detection technique. This work can be extended by using a classifier that can learn new attack types on the network. Research areas involving time optimization of the IDS can also be carried out.

REFERENCES

[1] Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, Ed., (2000): “State of the Practice of Intrusion Detection Technologies”.Technical Report. CMU/SEI-99-TR-028, Carnegie Mellon University, Software E

[2] Anderson, J. P., (1980): “Computer Security Threat Monitoring and Surveillance”. Fort Washington.PA Computer Security Resource Center.

[3] Denning, D. E. (1987): "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):pp. 222-232.

[4] Heberlein, L. et al.(1990): "A Network Security Monitor”. Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, pp. 296-303.

[5] Mchugh, J. et al. (2001): "Intrusion Detection: Implementation and Operational Issues" Software Engineering Institute Computer Emergency Response Team White Paper.

[6] Power Richard. (1999):“CSI/FBI Computer Crime and Security Survey". Computer Security Journal, Volume XV, Number 2, pp. 32.

[7] Proctor Paul (2000):“The Practical Intrusion Detection Handbook”. Prentice Hall.

[8] Mark Crosbie, Gene Spafford., (1994): "Defending aComputer System using Autonomous Agents". Technical report No. 95-022, COASTLaboratory, Department of Computer Sciences,Purdue University.

[9] S. R. Snapp et al., (1991): "A system for distributed intrusion detection", Proceedings of the IEEECOMPCON 91, San Francisco, CA.

[10] Joe Bowling (2003). “ISW Security Papers.Available athttp://www.infosecwriters.com/www.whitehats.com.

[11] ISS (Internet Security Systems) “The evolution of intrusion detection technology, 2001.Available online at http://documents.iss.net/whitepapers/TheEvolutionofIntrusionDetectionTechnology.pdf.

[12] Ross Anderson, (2004): Cambridge Computing labs, Information Security Group at http://www.cl.cam.ac.uk/~rja14/econsec.html

[13] AurobindoSundaram. (2005):“An Introduction to Intrusion Detection.CCNA: Cisco Certified Network Associate Study Guide Fourth Edition.

[14] Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick.(2001) “Intrusion Signatures and Analysis”. New Riders; ISBN: 0735710635 Intrusion Signatures and Analysis.

]15] Cothers, Tim (2003): “Implementing Intrusion Detection Systems”.A Hands-On Guide for Securing the Network. Available at http://www.ebay.com/ctg/Implementing-Intrusion-Detection-Systems-Hands-On-Guide-Securing-Network-Tim-Crothers-2002-Paperback-/2304802

[16] Dragon (2004). Dragon by Security Wizards http://www.network-defense.comhttp://www.enterasys.com/home.html

[17] Etrust(2004):eTrust Intrusion Detection by Computer Associates

http://www.ca.com/Solutions/Product.asp?ID=163

[18] Fidelis (2009).Fidelis Security System. Available athttp://www.fidelissecurity.com/

[19] Frincke Deborah (2003): “Balancing Cooperation and Risk in Intrusion Detection”.University of Idaho SIGKDD. Washington, DC, USA.

[20] Graham, Robert“Network Intrusion Detection Systems” http://www.robertgraham.com/pubs/network-intrusion-detection.html

[21] Infosecurity Management 2002 Vendor conference on Managing Security Risks can be seen at the following URL. http://www.infosecuritymanagement.com/index

[22] Andy Cuff (2003): “Intrusion Detection Terminology”(Part One). Available athttp://www.symantec.com/connect/articles/intrusion-detection-terminology-part-one

[23] Internet Security Systems (ISS).“The evolution of intrusion detection technology Aug 29,2001http://documents.iss.net/whitepapers/The Evolution of Intrusion Detection Technology.pdf

[24] Otey M.,Parthasarathy S., Ghoting A, Li G.,Narawula S., Panda D. (2003): “Towards NIC based Intrusion Detection”. Available at http://www.cse.ohio-state.edu/dmrl/papers/kdd03.pdf

[25] Marty Rosech(2003): CEO of Sourcefire, Seminar on the Future of IDS. Washington DC. Available at http://www.infosecwriters.com/texts.php?op=display&id=115

[26] EinwechterNathan(2002): “An Introduction To Distributed Intrusion Detection Systems. Available at http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems

[27] Robert Graham (Security consultant). Available at http://www.robertgraham.com/pubs/network-intrusion-detection.html