SIGNIFICANCE & APPLICATIONS OF INTRUSION DETECTION SYSTEM (IDS)

[1]kalyan Kumar Dasari, [2] Dr.E.Srinivasa Reddy

[1]*Research scholar, Department of Computer Science & Engineering, Acharya Nagarjuna University, AP, India,* ***dkkumar123@gmail.com***

[2] *Professors, Department of Computer Science & Engineering, Acharya Nagarjuna University, AP, India,* ***edara_67@yahoo.com.***

Abstract: *Attackers computers, who are extend across the Internet have become a main threat in our world, The research scholars proposed many number of techniques and mechanisms such as (firewall, encryption etc..) to prevent such diffusion and protect the infrastructure of computers, but with this, the attackers managed to enter the computers. IDS has taken much of the attention of research scholars, IDS looking up the assets of computer and sends reports on the activities of any anomaly or extraordinary patterns. The aim of this paper is to explain the different steps of the evolution of the idea of IDS and its significance to research scholars and research centers, security, military and to observe the importance of intrusion detection systems and categories , classifications, and where can put IDS to reduce the risk to the network.*

Keywords*: Intrusion Detection System (IDS), classifications of IDS, NID*

INTRODUCTION

Security is an important subject for all the networks of companies, organizations and education institutions at the present instance and all the intrusions are trying in ways that successful access to the data network of these companies and Web services and despite the development of many ways to ensure that the permeation of intrusion to the infrastructure of the network via the Internet, through the use of firewalls, encryption, etc. But intrusion detection system (IDS) is a relatively new technology of the techniques for intrusion detection methods that have emerged in recent years.

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within 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). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

6 Steps for Effective Information Security Assessments

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

The purpose of IDS is to help computer systems on how to deal with attacks, and that IDS is collecting information from several different sources within the computer systems and networks and compares this information with pre-Existing patterns of discrimination as to whether there are attacks or weaknesses.

INTRUSION DETECTION SYSTEMS: A BRIEF HISTORY

The goal of intrusion detection is to monitor network assets to detect anomalous behavior and misuse in network. This concept has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity and incorporation into the overall information security infrastructure. Beginning in 1980, with James Anderson's paper, Computer Security Threat Monitoring and Surveillance, the intrusion detection was born. Since then, several polar events in IDS technology have advanced intrusion detection to its current state.

James Anderson's seminal paper, was written for a government organization, introduced the notion that audit trails contained vital information that could be valuable in tracking misuse and understanding of user behavior. With the release of this paper, the concept of "detecting" misuse and specific user events emerged. His insight into audit data and its importance led to tremendous improvements in the auditing subsystems of virtually every operating system. Anderson's hypothesize also provided the foundation for future intrusion detection system design and development. His work was the start of host-based intrusion detection and IDS in general.

In 1983, SRI International, and Dr. Dorothy Denning, began working on a government project that launched a new effort into intrusion detection system development. Their goal was to analyze audit trails from government mainframe computers and create profiles of users based

Upon their activities. One year later, Dr. Denning helped to develop the first model for intrusion detection, the Intrusion Detection Expert System (IDES), which provided the foundation for the IDS technology development that was soon to follow.

In 1984, SRI also developed a means of tracking and analyzing audit data containing authentication information of users on ARPANET, the original Internet. Soon after, SRI completed a Navy SPAWAR contract with the realization of the first functional intrusion detection system, IDES. Using her research and development work at SRI, Dr. Denning published the decisive work, An Intrusion Detection Model, which revealed the necessary information for commercial intrusion detection system development. Her paper is the basis for most of the work in IDS that followed. The subsequent iteration of this tool was called the Distributed Intrusion Detection System (DIDS). DIDS augmented the existing solution by tracking client machines as well as the servers it originally monitored. Finally in 1989, the developers from the Haystack project formed the commercial company, Haystack Labs, and released the last generation of the technology, Stalker. Crosby Marks says that "Stalker was a host-based, pattern matching system that included robust search capabilities to manually and automatically query the audit data." The Haystack advances, coupled with the work of SRI and Denning, greatly advanced the development of host-based intrusion detection technologies.

Commercial development of intrusion detection technologies began in the early 1990s. Haystack Labs was the first commercial vendor of IDS tools, with its Stalker line of host-based products. SAIC was also developing a form of host-based intrusion detection, called Computer Misuse Detection System (CMDS). Simultaneously, the Air Force's Crypto logic Support Canter developed the Automated Security Measurement System (ASIM) to monitor network traffic on the US Air Force's network. ASIM made considerable progress in overcoming scalability and portability issues that previously plagued NID products. Additionally, ASIM was the first solution to incorporate both a hardware and software solution to network intrusion detection. ASIM is still currently in use and managed by the Air Force's Computer Emergency Response Team (AFCERT) at locations all over the world. As often happened, the development group on the ASIM project formed a commercial company in 1994, the Wheel Group. Their product, Net Ranger, was the first commercially viable network intrusion detection device.

The intrusion detection market began to gain in popularity and truly generate revenues around 1997. In that year, the security market leader, ISS, developed a network intrusion

detection system called Real Secure. A year later, Cisco recognized the importance of network intrusion detection and purchased the Wheel Group, attaining a security solution they could provide to their customers. Similarly, the first visible host-based intrusion detection company, Centrex Corporation, emerged as a result of a merger of the development staff from Haystack Labs and the departure of the CMDS team from SAIC. From there, the commercial IDS world expanded its market-base and a roller coaster ride of start-up companies, mergers, and acquisitions ensued.

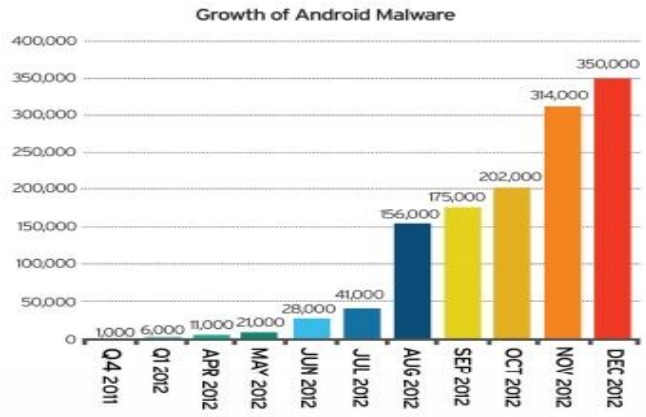


Figure 1: Number of incidents reported

The above chart from US-CERT shows how the cyber incidents rose in current internet network environment; this gives requirement of IDS deployment in network security model.

Network intrusion detection actually deals with information passing on the wire between hosts. Typically referred to as "packet-sniffers," network intrusion detection devices intercept packets travelling in and out in network along various

communication mediums and protocols, usually TCP/IP. Once captured, the packets are analyzed in a number of different ways. Some IDS devices will simply compare the packet to a signature database consisting of known attacks and malicious packet "fingerprints", while others will look for anomalous packet activity that might indicate malicious behavior.

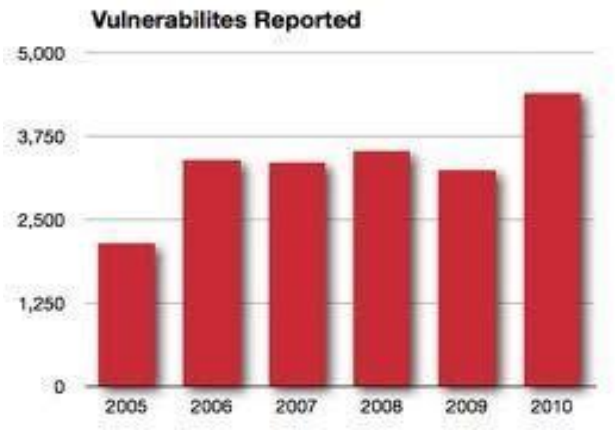


Figure 2: Vulnerabilities reported

The IDS basically monitors network traffic for activity that falls within the banned activity in the network. The IDS main job is gives alert to network admin for allow them to take corrective action, blocking access to vulnerable ports, denying access to specific IP address or shutting down services used to allow attacks. This is nothing but front line weapon in the network admin war against hackers.

Categories of intrusion detection system

Intrusion detection system is classified into three categories: signature based detection systems, anomaly based detection systems and specification based detection systems.

1. Signature based detection systems

Signature based detection system (also called misuse based)
, This type of detection is very effective against known attacks, and it depends on the receiving of regular updates of patterns and will be unable to detect unknown previous threats or new releases.

2. Anomaly based detection system

This type of detection depends on the classification of the network to the normal and anomalous, as this classification is based on rules or heuristics rather than patterns or signatures and the implementation of this system we first need to know the normal behavior of the network.

Anomaly based detection system unlike the misuse based detection system because it can detect previous unknown threats, but the false positive to rise more probably.

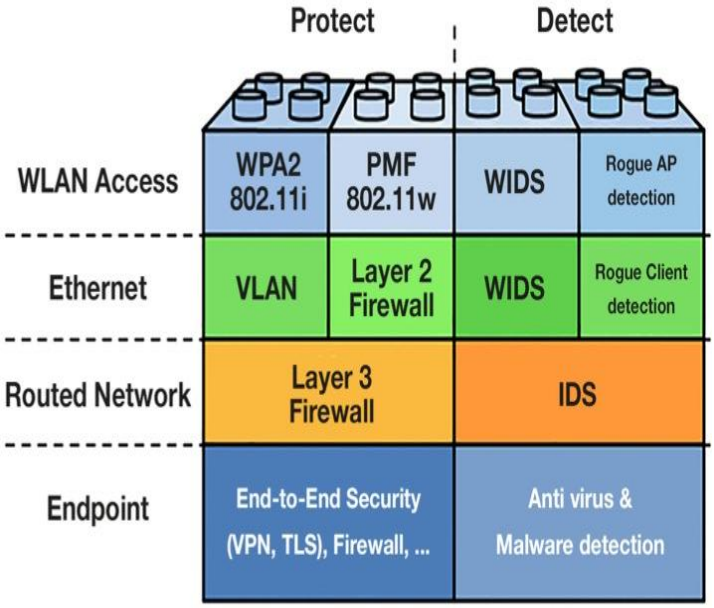
3. Specification based detection system

This type of detection systems is responsible for monitoring the processes and matching the actual data with the program and in case of any Abnormal behavior will be issued an alert and must be maintained and updated whenever a change was made on the surveillance programs in order to be able to detect the previous attacks the unknown and the number of false positives what can be less than the anomaly detection system approach.

CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion detection system are classified into three types

1. Host based IDS
2. Network based IDS
3. Hybrid based IDS



1. Host based IDS (HIDS)

A host-based IDS is capable of monitoring all or parts of the dynamic behavior and the state of a computer system, based on how it is configured. Besides such activities as dynamically inspecting network packets targeted at this specific host (optional component with most software solutions commercially available), a HIDS might detect which program accesses what resources and discover that, for example, a word-processor has suddenly and inexplicably started modifying the system password database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.

2. Network based IDS (NIDS)

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats. A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network. Hybrid based IDS

3. Hybrid based IDS

We have examined the different mechanisms that different IDSs use to signal or trigger alarms on your network. We have also examined two locations that IDSs use to search for intrusive activity. Each of these approaches has benefits and drawbacks. By combining multiple techniques into a single hybrid system, however, it is possible to create an IDS that possesses the benefits of multiple approaches, while overcoming many of the drawbacks.

Although it is true that combining multiple different IDS technologies into a single system can theoretically produce much stronger IDS, these hybrid systems are not always better systems. Different IDS technologies examine traffic and look for intrusive activity in different ways. The major drawback to a hybrid IDS is getting these different technologies to interoperate successfully and efficiently. Getting multiple IDS approaches to coexist in a single system can be a very challenging task

CONCLUSION

An intrusion detection system is a part of the defensive Operations that complements the defenses such as firewalls, UTM etc. The intrusion detection system basically detects attack signs and then alerts. According to the detection methodology, intrusion detection systems are typically categorized as misuse detection and anomaly detection systems. The deployment perspective, they are be classified in network based or host based IDS. In current intrusion detection systems where information is collected from both network and host resources. In terms of performance, an intrusion detection system becomes more accurate as it detects more attacks and raises fewer false positive alarms.

REFERENCES

[1] Anderson, James P., “Computer Security Threat Monitoring and
Surveillance”,Fort Washington, Pa., 1980.

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

[3] Heberlein, L. etal. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp.296-303.

[4] Paul Innella Tetrad, “The Evolution of Intrusion Detection Systems”, Digital Integrity,LLC on November 16, 2001.

[5] Harley Kozushko, “Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems”, on September 11, 2003.

[6] "DOD 5200.28-STD National Computer Security Center", *Trusted Computer System Evaluation Criteria*, Dec. 1985.

[7] "DOD 5200.28-STD National Computer Security Center", *Trusted Computer System Evaluation Criteria*, July 1987.

[8] W. T. Tener, "AI&4GL: Automated Detection and Investigation Tools", *Proc. Fifth IFIP International Conference on Computer Security*, 1988-May.

[9] H. S. Javitz, A. Valdez, "The SRI IDES Statistical Anomaly Detector", *Proc. 1991 IEEE Symposium on Research in Security and Privacy*, 1991-May.

[10] C. Dowell, P. Ramstedt, "The COMPUTERWATCH data reduction tool", *Proc. 13th National Computer Security Conference*, pp. 99-108, 1990-Oct.

[11] W. T. Tener, "Discovery: an expert system in the commercial data security environment", *Proc. Fourth IFIP TC11 International Conference on Computer Security*, 1986-Dec.

[12]T. F. Lunt, "IDES: A Progress Report", *Proc. Sixth Annual*

Computer Security Applications Conf., 1990-Dec.

[13] T. F. Lunt, *A Real-time Intrusion Detection Expert System (IDES)*, May 1990.

[14] J. R. Winkler, W. J. Page, "Intrusion and Anomaly Detection in Trusted Systems", *Proc. Fifth Annual Computer Security Applications Conference*, 1989-Dec.

[15] S. M. Bellovin, "Security problems in the TCP/IP protocol suite", *ACM Computer Commun. Review*, vol. 19, no. 2, pp. 32-48, April 1989.

[16]H. S. Teng, K. Chen, S. C.-Y. Lu, "Adaptive real-time anomaly detection using inductively generated sequential patterns", *Proc. 1990 Symposium on Research in Security and Privacy*, 1990-May.

[17]S. R. Snapp, B. Mukherjee, K. N. Levitt, "Detecting intrusions through attack signature analysis", *Proc. 3rd Workshop on Computer Security Incident Handling*, 1991-Aug.

[18]S. R. Snapp, *Signature Analysis and CommunicationIssuesin a Distributed Intrusion Detection System*, University of California, Aug. 1991.

[19]J. Doak, *Intrusion Detection: The Application of Feature Selection a Comparison of Algorithms and the Application of a Wide Area Network Analyzer*, University of California, August 1992.

[20] L. T. Hebertein, *Towards Detecting Intrusions in a Networked Environment*, University of California, June 1991.

[21] L. T. Heberlein, "Towards detecting intrusions in a networked environment", *Proc. 14th DOE Conference on Computer Security*, pp. 17-47-17-65, 1991-May.

[22]L. T. Heberlein, K. N. Levitt, B. Mukherjee, "A method to detect intrusive activity in a networked environment", *Proc. 14th National Computer Security Conference*, pp. 362-371, 1991-Oct.

[]23T. Bartoletti, "SPI/UNIX: Security Profile Inspector for UNIX computer systems", *Proc. 3rd Workshop on Computer Security Incident Handling*, 1991-Aug.

[24] S. R. Snapp, "A system for distributed intrusion detection", *Proc. IEEE COMPCON 91*, pp. 170-176, 1991-Feb.

[25]S. R. Snapp, "DIDS (Distributed Intrusion Detection System) — Motivation Architecture and An Early Prototype", *Proc. 14th National Computer Security Conf.*, 1991-Oct.

ABOUT THE AUTHOR:

1. Mr. Kalyan Kumar Dasari is research scholar, department of computer science & engineering, Acharya Nagarjuna University. dkkumar123@gmail.com.

2. Dr. E. Srinivasa Reddy is working as a professor in the department of computer science & engineering, at Acharya Nagarjuna University. edara_67@yahoo.com.