IMPORTANCE OF INTRUSION DETECTION SYSTEM ON DIFFERENT INTRUSION ATTACKS

Author[1]: Dr Mehul Patel, Assistant Professor
S.G.M. English Medium College of Commerce and Management, (SEMCOM)
The CVM University, Vallabh Vidyanagar, Gujarat

Author[2]: Mr. Abhishek Dave, Assistant Professor
S.G.M. English Medium College of Commerce and Management, (SEMCOM)
The CVM University, Vallabh Vidyanagar, Gujarat

ABSTRACT:

Intruders computers, which are spread across the web, have become a serious threat to our world. IDS takes great care of researchers, monitors IDS resources on a computer and sends reports on any inconsistent or bizarre pattern of activity. The purpose of this paper is to describe the evolutionary stages of IDS thinking and researchers and research centres, security, the military and its intrusion detection system and classes, to examine the importance of classification and where IDS can be placed. Scale the danger back on the network.

Keywords: Intrusion detection, IDS, variance & abuse, NID

INTRODUCTION

Intrusion Attack

Computer intrusion occurs when someone tries to gain access to any part of your computer system. Computer intruders or hackers usually use automated computer programs when they try to compromise computer security. An intruder can try many ways to gain access to your computer. They can:

1. Access your computer to view, change or delete information on your computer.

2. Crash or slow down your computer.

3. Access your private data by checking the files on your system.

4. Use your computer to access other computers on the Internet.

Intrusion Attack Reports Dashboard provides insight into attack attempts in your network.

The reports provide complete statistics about the attacks and the attackers including brief reports on the victims and the programs through which the attack was initiated.

These reports can make it easier for administrators to determine the severity of an attack and thus provide a basis for optimizing intrusion prevention policies.

View the Dashboard of Attack Reports from Monitoring and Analysis> Reports> Networks and Threats> Intrusion Attacks.

It enables the breakdown of various attacks to look like this:

1. Attack categories

2. Attack platform

3. Attack targets

4. Severity wise attacks

5. Infiltration attacks

6. Attacks have been detected

7. Source of infiltration

8. Intrusion target

9. Users

10. Applications used for Attacks

11. Source countries

12. Attitude - Infiltration attacks

Intrusion Detection System

Security is currently an important issue for all networks of companies and organizations and all intruders are trying to gain successful access to the data networks of these companies and web services and despite the development of many ways to ensure intrusion through the Internet, fires, encryption. Intrusion into network infrastructure through the use of.

But IDS is a relatively new set of techniques for intrusion detection methods that have emerged in recent years. The main role of the network of intrusion detection systems is to help computer systems prepare and deal with network attacks.

Infiltration investigations include:

1. Monitor and analyse user and system activities
2. Analysis of system configurations and vulnerabilities
3. Evaluate system integrity and file integrity
4. Attacks Ability to identify specific patterns of attacks
5. Activity Analysis of abnormal activity patterns
6. Policy Tracking of user policy violations

IDS aims to help computer systems learn how to deal with attacks, and it collects and compares information from many different sources in IDS computer systems and networks.

Existing methods of discrimination on whether there are attacks or vulnerabilities IDS aims to help computer systems deal with attacks, and that IDS is collecting information from many different sources in computer systems and networks and comparing this information with the former. doing.

Existing methods of discrimination regarding whether there are attacks or vulnerabilities.

A HISTORY:

The goal of detecting intrusion is to monitor network assets to detect abnormal behaviour and abuse in the network. The concept has been around for almost twenty years, but only recently has it dramatically increased in popularity and incorporated into the overall information security infrastructure. In 1980, intrusion detection was born from James Anderson's paper, Computer Security Threat Monitoring and Surveillance. Since then, several polar events in IDS technology have investigated intrusion into its current state.

James Anderson's half-paper, written for a government agency, introduced the notion that audit trails contain important information that could be valuable in understanding abuse and user behaviour. With the publication of this paper, the concept of "discovering" abuse and specific user events emerged. Their understanding of audit data and its importance led to tremendous improvements in the dating subsystems of virtually every operating system. Anderson’s hypothesis also provided the foundation for future intrusion detection STM design and development. His work was host-based intrusion investigations and the introduction of IDS in general.

In 1983, SRI International, and Dr. Dorothy Denning, began working on a government project that launched a new effort in the development of an infiltration investigation system. Their goal was to analyse audit trails from government mainframe computers and create user profiles based

On their activities. A year later, De Den Ning helped develop the first model for intrusion detection of the Intrusion Detection Expert System (IDES), which laid the groundwork for the upcoming IDS technological development.

In 1984, SRI also developed a means of tracking and analysing audit data containing authentication information of users on the original Internet, ARPNET. Soon, SRI completed the Navy Spare Agreement with the realization of the first functional intrusion detection system, IDES. Using his research and development work at SRI, Dr. Denning published a critical work, an intrusion detection model, which revealed the information needed for the development of a commercial intrusion detection system. Her paper is the basis for most of the subsequent IDS work. The subsequent iteration of this tool is called Distributed Intrusion Detection System (DIDS). DIDS has enhanced the existing solution by tracking client machines as well as the servers it originally monitors. Finally, in 1989, the developers of the Hastack project created a trading company, Hastack Labs, and introduced the last pay generation of Technologies, the Stalker. "Stalker was a host-based, pattern-matching system with strong search capabilities for manually and automatically querying audit data," says Crossby Marks. With the work of Hastack Advances, SRI and Denning, the development of host-based intrusion detection technologies has progressed greatly.

Commercial development of infiltration detection technologies began in the early 1990s. Hastack Labs was the first commercial vendor of IDS tools, with a stalker line of its host-based products. SAIC was also developing a type of host-based intrusion detection called the Computer Muse Detection System (CMDS). Simultaneously, the Air Force's Crypto Logic Support Center developed the Automotive Security Measurement System (ASIM) to monitor network traffic on the U.S. Air Force's network. ASIM made significant progress in eliminating issues of scalability and portability that previously plagued NID products. In addition, ASIM was the first solution to include both hardware and software solutions for network intrusion detection. ASIM is currently used and operated by the Air Force's Computer Emergency Response Team (AFCERT) at locations around the world. As has often been the case, the development group on the ASIM project formed a business company,

Wheel Group, in 1994. Their product, the Net Ranger, was the first commercially capable country network intrusion detection device.

Infiltration investigations began to gain popularity in the market and around 1997 began to generate real revenue. In that year, the security market leader developed ISSA network infiltration.

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

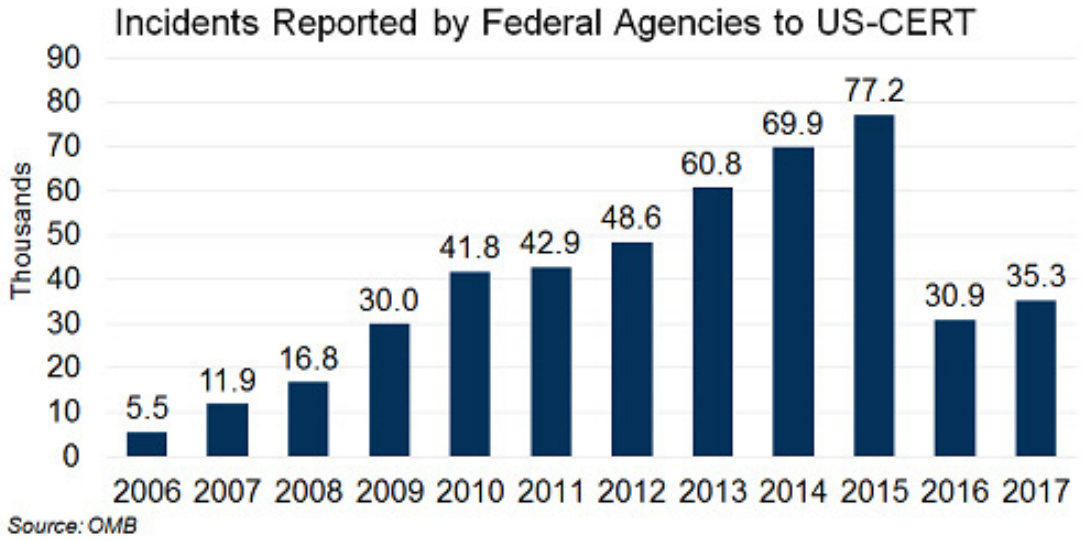

Figure 1: Number of reported incidents

The above chart of US-CERT shows how cyber incidents have increased in the current Internet network environment. This requires the deployment of IDS in the network security model.

Network intrusion detection actually deals with information passing over wires between hosts. Commonly referred to as "packet-sniffers," network intrusion detection devices intercept packets that travel across a network with a variety of communication media and protocols, usually TCP / IP. Once captured, the packets are analysed in a variety of ways.

Some IDS devices will only compare packets with known attacks and a signature database containing malicious packet "fingerprints", while others will look for incompatible packet activity that may indicate malicious behaviours.

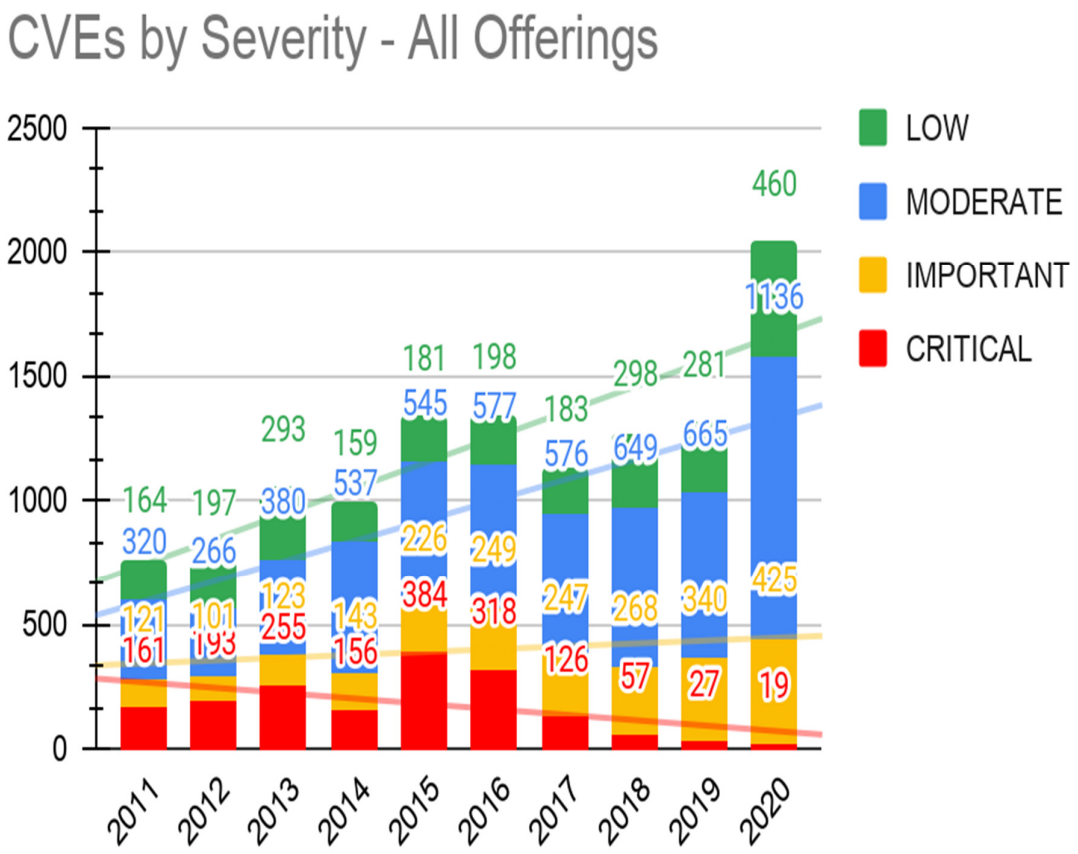

Figure 2: Report vulnerabilities

IDS basically monitors network traffic for the activity that occurs in the restricted activity in the network. The main function of IDS is to alert network admins to allow corrective action, to block access to vulnerable ports, to deny access to specific IP addresses, or to shut down services used to allow attacks. This network is nothing but a front line weapon, waging a war against hackers. This information is then compared with predefined blueprints of known attacks and vulnerabilities.

Categories of intrusion detection system

Intrusion detection systems are classified into three categories: signature-based search systems, inconsistency-based search systems, and specification-based search systems.

1. **Signature based inspection systems**

Signature based investigation system (also called abuse based)

This type of investigation against known attacks is very effective, and it is based on receiving regular updates of the pattern and will not detect previously unknown threats or new releases.

2. **Incompatibility based search system**

This type of search is based on the classification of general and inconsistencies of the network, as this classification is based on rules or heuristic sticks rather than patterns or signatures and for the implementation of this system we first need to know the general behaviour of the network.

The contrast-based search system is unlike the abuse-based detection system because it can detect previously unknown threats, but the false positives continue to grow.

3. **Specification based investigation system**

This type of investigation system is responsible for monitoring processes and matching the actual data with the program and will be alerted in case of any abnormal behaviour and must be maintained and updated when any changes are made to the surveillance programs. Previous attacks have been able to detect a number of unfamiliar and false positives that may be less than the approach of the inconsistency detection method.

Classification of Intrusion Detection System

Intrusion detection systems are classified into three types

1. Host based IDS

2. Network based IDS

3. Hybrid based IDS

1. Host based IDS (HIDS)

This type is placed on a device such as a server or workstation, where the data is analysed locally on the machine and this data is collected from various data. HIDS Both inconsistent and abusive can use the search system.

2. Network Based IDS (NIDS)

NIDS is deployed at strategic points in the network infrastructure. NIDS can capture and analyse data to detect known attacks by comparing examples or signatures from a database or scanning traffic for inconsistent activity to detect illegal activities. NIDS are also known as "packet-sniffers" because they capture packets passing through the media.

3. Hybrid based IDS

Management and alerting of both network and host-based intruder detection devices, and NID and HID - provide logical complements to central intrusion detection management.

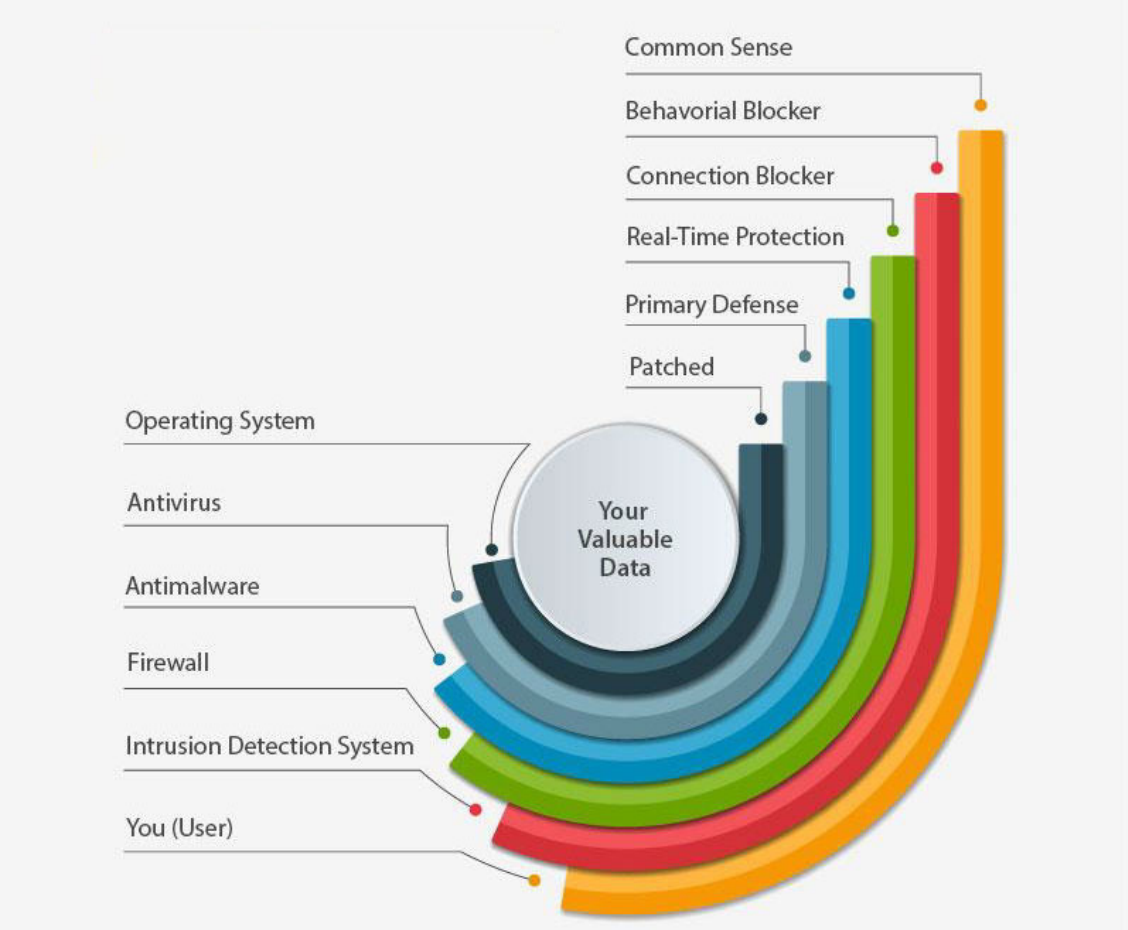

Figure3: Layered Security approach for reducing risk

CONCLUSION

An intrusion detection system is part of a protective operation that completes defense such as firewalls, UTMs, etc. The intrusion detection system basically detects signs of an attack and then alerts. According to the search method, intrusion detection systems are generally classified as abuse detection and inconsistency detection systems. Deployment perspective, they are classified into network based or host based IDS. In current intrusion detection systems where information is collected from both network and host sources. In terms of performance, the intrusion detection system becomes more accurate as it detects more attacks and generates 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. https://docs.sophos.com/nsg/sophos-firewall/v17.0.0/Help/en-us/webhelp/onlinehelp/index.html#page/onlinehelp/reportgroupid900000.html