Survey on Intrusion Detection System

Jalpa M. Gandhi

Student (Master of Engineering)
Computer Engineering,
Alpha College of Engineering and Technology, Ahmedabad, India
jalpamgandhi@gmail.com

***Abstract*—Intrusion Detection System is one that detects unauthorized user or unauthorized activity of authorized author. Main purpose of this system is to find out behavior anomalies because of which user impersonations can be detected. Variety of techniques is used for this which is described in this paper. In this article, we will see some basic concepts of the system**

***Index Terms*—Working of IDS, Types of IDS, Types of alerts, Techniques, Parameters**

I. INTRODUCTION

The computing world has been changed a lot recently because of the progress of the World Wide Web. In this, the information and resources are shared between the computers in the network. But this type of sharing needs some security mechanisms. This is because in the highly interconnected networks also have unauthorized persons or users, there should be some restrictions for accessing shared information and resources. Therefore, anybody does not have permission can't access them. For this, tools like firewalls, anti-virus systems, intrusion detection system, etc are developed. Due to higher complexity of attack and networks, most commonly used tool is intrusion detection system.

II. WORKING OF IDS

Intrusion Detection System is guard a system which detects and responds to malicious traffic in the network and misuse of the computer. Intrusion detection is a process of identifying and responding to malicious/unauthorized activities.

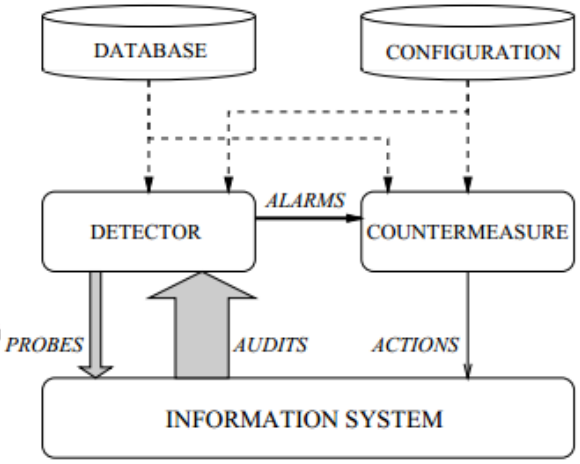

Figure 1: Architecture of IDS [2]

Architecture of intrusion detection system is shown in the figure above. Main purpose of the system is to detect computer attacks and computer misuse, and to provide notification to the proper individuals when detection. This system that is installed on a network serves the same purpose as a burglar alarm system installed in a house serves [1] [6] [7] [8].

An intrusion detection system in core is a detector which processes the information imminent to be protected from the system. This detector mainly launches probes to trigger the process like requesting version number of applications. Main aim of this detector is to remove not needed information from the process / audit trail. Then it presents synthetic view of the current security state of the system. Based on this view decision is taken to measure the possibility of intrusion. After that, corrective action (which is to prevent the actions from being executed or to change the state of the system back to the secure state) can be taken.

There are some common steps that IDS follows. They are listed below,

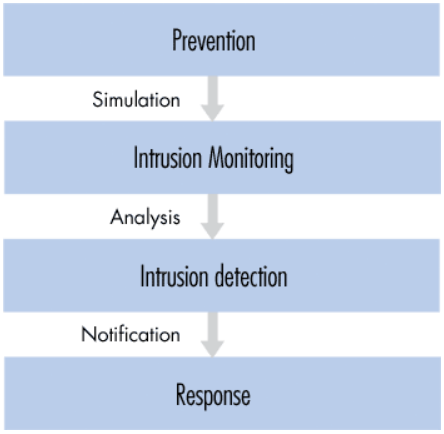

Figure 2: Steps followed by IDS [4]

- ✓ First capture data which is mostly in the form of IP packets.
- ✓ Then decode that captured data and transform it into a unique format. For this feature extraction method can be used.
- ✓ Now analysed and classify (whether it is authorized or not) that data in a manner such that it is specific to the individual IDS.
- ✓ Further generate alerts if an unauthorized activity is detected.

III. TYPES OF IDS

Intrusion Detection System can be divided into two types as shown below [2],

1. Host based IDS (HIDS): This system examines data held on individual computers that serve as hosts. It collects and analyzes data that originate on a computer that hosts a service. Once this data is aggregated for a given computer, it can either be analyzed locally or sent to a separate/central analysis machine. This type of system also efficient to detect unauthorized modification of file
2. Network based IDS (NIDS): This system examines data exchanged between computers. It analyzes data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify their nature. Instead of analyzing information that originates and resides on a computer, network-based IDS uses techniques like "packet-sniffing" to pull data from TCP/IP or other protocol packets traveling along the network [9]. Commonly this system is best to detect following activities,
   - ✓ Unauthorized outsider access.
   - ✓ Bandwidth theft/denial of service.

HIDS and NIDS differ significantly from each other but complement one another. The network architecture of host-based is agent-based, which means that a software agent resides on each of the hosts that will be governed by the system. In addition, more efficient host-based intrusion detection systems are capable of monitoring and collecting system audit trails in real time as well as on a scheduled basis, thus distributing both CPU utilization and network overhead and providing for a flexible means of security administration. In a proper IDS implementation, it would be advantageous to fully integrate the network intrusion detection system, such that it would filter alerts and notifications in an identical manner to the host-based portion of the system, controlled from the same central location. In doing so, this provides a convenient means of managing and reacting to misuse using both types of intrusion detection. That said, as an organization introduces an IDS into its network to augment its current information security strategy, the primary focus of the intrusion detection system should be host-based.

Although network intrusion detection has its merits and certainly must be incorporated into a proper IDS solution, it has historically been incapable of evolving to comply with the growing technology of data communications. Most NIDS perform miserably, if at all, on switched networks, fast networks of speeds over 100 Mbps, and encrypted networks. Furthermore, somewhere in the range of 80 to 85 percentage of security incidents originate from within an organization. Consequently, intrusion detection systems should rely predominantly on host-based components, but should always make use of NIDS to complete the defenses. In short, a truly secure environment requires both a network and host-based intrusion detection implementation to provide for a robust system that is the basis for all of the monitoring, response, and detection of computer misuse.

IV. TYPES OF ALERTS

There are mainly four types of alerts provided by IDS [5].

1. True positive: Detects and notifies user when attack is done.
2. True negative: Does not notify user when no attack presents.
3. False positive: Detects and notifies user when no attack presents.
4. False negative: Does not detect attack.

V. TECHNIQUES USED IN IDS

Basically, there are main four techniques used to detect unauthorized user or unauthorized access of user and they are anomaly detection, misuse detection, target monitoring and stealth probes [1] [3] [5].

1. Anomaly Detection: In this technique, the system is designed such a way that it uncovers unusual patterns of behavior. Here, the system establishes a line of usual patterns of behavior. Any behavior of user which differs broadly from that line is notified as a possible intrusion. An example of this would be if a user uses a computer at 6:00 AM which is not come in business hours and at this time nobody has access. Therefore this should raise possibility of intrusion. So the system can properly alert its administrators.
2. Misuse/Signature Detection: In this technique, the system stores the unusual patterns of unauthorized activities. So that it can determine and detect similar kind of attempts. These specific patterns are called signatures. Therefore this technique is also known as signature detection. An example of this is "three failed logins" at an ATM center of the bank. The incident of a signature may not signify that an actual unauthorized access is attempted, but it is good to take each alert seriously. Depending on the robustness and seriousness of a signature, the alert is triggered to the proper authorities.
3. Target Monitoring: In this, the systems look for the alteration of specified files instead of searching for the patterns of usual or unusual behavior of the user continuously. This is more of a corrective control which is designed to uncover an unauthorized action after it occurs, so that the action can be reversed. This system is easy to implement as it does not require continuous monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files.
4. Stealth Probes: This technique attempts to detect that any attackers choose to carry out their mission over prolonged periods of time. For an example, intruders will check for weaknesses in the system and open ports over a period, and wait for the same period to actually launch the attacks. This collects various data throughout the system and then checks for any methodical attacks over a long period of time. They take big area for sampling and attempt to discover any correlating attacks. Thus, this method is combination of anomaly detection and misuse detection methods in order to detect suspicious activity.

VI. PARAMETERS OF IDS

There are various parameters listed below are used to measure performance of the system [1].

- ✓ Accuracy: This is ability of the system to detect attacks properly and also ability to produce false alerts. Inaccuracy occurs when a system detects a usual activity in the environment as suspicious.
- ✓ Performance: This is ability of the system to process the events. If this is poor in the system, then there is no possibility of real time detection.
- ✓ Completeness: This is ability of the system to detect all the attacks. Incompleteness occurs when the system fails to detect an attack. This is very difficult to estimate because it is not possible to have knowledge about all the possible attacks.
- ✓ Fault tolerance: This is ability of the system to resist the attacks.
- ✓ Timeliness: This considers the internal processing speed of the system and the time required to spread the information and respond to it. So this is more important than the performance of the system.

VII. CONCLUSION

Intrusion Detection System is a part of active research because now a day, computer systems are highly interconnected with one another in order to share the information and because of that the possibility of unauthorized activity increases. Therefore, this paper includes brief description about Intrusion Detection System, its architecture, types of alerts provided by it, its performance parameters.

REFERENCES

[1] Paul Innella, "An Introduction to IDS", http://www.symantec.com/connect/articles/introduction-ids.

[2] Herve Debar, "An introduction to IDS", IBM Research - Switzerland, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.7433&rep=rep1&type=pdf.

[3] Huwaida Tagelsir Elshoush and Izzeldin Mohamed Osman, "Alert correlation in collaborative intelligent intrusion detection systems – A survey", http://www.sciencedirect.com/science/article/pii/S156849461000311.

[4] Przemyslaw Kazienko & Piotr Dorosz, "Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks and IDS architecture)", http://www.systemcomputing.org/ssm10/intrusion_detection_systems_architecture.htm.

[5] E. Lundin, E. Jonsson, "Survey of research in the intrusion detection area", Technical report 02-04, Department of Computer Engineering, Chalmers University of Technology, Göteborg, http://www.ce.chalmers.se/staff/emilie/papers/Lundin_survey02.pdf.

[6] H. Debar, M. Dacier, A. Wespi, "Towards a taxonomy of intrusion-detection systems", Computer Networks.

[7] G. Mansfield, K. Ohta, Y. Takei, N. Kato, Y. Nemoto, "Towards trapping wily intruders in the large", Computer Networks.

[8] P. Dorosz,P. Kazienko,Systemy wykrywania intruzów,VI Krajowa Konferencja Zastosowan Kryptografii ENIGMA, Warsa, http://www.enigma.com.pl/konferencje/vi_kkzk/index.htm.

[9] B. Mukherjee, T.L. Heberlein, K.N. Levitt, "Network intrusion detection", IEEE Network 8.