Intrusion Detection Systems: Principles And Perspectives

[1]Mohammed Jamal al-mansor
Department of Electrical, Electronic and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Malaysia
Email: m_j_2006_2009@yahoo.com

[1]Kok Beng Gan
Department of Electrical, Electronic and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Malaysia
Email: gan kokbeng@ukm.edu.my

Abstract— **Intrusion detection systems have gained large interest in securing networks information for the last decade. Most recently proposed security approaches such as layered defense approach and defense in depth approach are based on intrusion detection systems as the key stone to provide high security levels. In this paper, we discuss the basic concepts of intrusion detection systems techniques in terms of their principle of work, advantages and disadvantages, also we compare the efficiency of these techniques in order to define the best approach.**

Keywords—Network security; intrusion detection systems; Security tools.

I. Introduction

Over the last decade, increased use of information technology in different organizations has led to increased needs in network security implementation . Computer networks that contain multi billion dollars information has been threatened by cyber criminals around the world. Traditional security mechanisms such as firewalls and encryption techniques, are facing huge challenges as the attackers develop more complicated attacks which sometimes can't be even detected. Using single stage protection cannot provide effective solution to secure organization networks, hence more sophisticated approaches were built to enhance the security. Layered defense approach [1, 2] is the most efficient approach introduced to provide total network security. However, the approach suggests to use hybrid security techniques in achieving effective protection. Intrusion detection systems (IDS), are one of the most important techniquesthe layered defense approach adopted. As most attacks require to compromise networks authentication and authorization first to provide an authorized access to the network resources, detecting the intrusion process is the first step towards defending organization network against any attack. Intrusion detection systems are normally used to detect the attacks and raise alarms to notify the defenders. In this paper, we discuss the basic concepts of intrusion detection systems in terms of their principle of work, advantages and disadvantages, and also what are the available types of these systems. The paper is organized as follows; section 1 includes classification of the most popular intrusion attacks, in section 2 we provide the basic principle of work of IDSs. In Section 3 we explain different types of intrusion detection systems, finally in section 4 we mention the most common known IDS tools.

II. Intrusion Attacks Classification

According to the literature [3-6], the most famous intrusion attacks can be classified as follows:

A. Denial of service attacks

In this case, the attacker employ series of mechanisms which aims to make the network resources unable to respond to the legitimate user requests, and thus leading to bring the network service dawn. Some of the attacks leading to deny authorized user to access the service. Most famous DoS attacks are: Ping of death, smurf and tear drop.

B. User to root attacks

The attacker gains root access to the system by exploiting systems vulnerability starting from normal user account. The attack is achieved through password sniffing or dictionary attack to reveal vulnerability points in the system, which allow the attacker to have root access to the system.

C. Remote to local attacks

In this attack, the attacker aims to achieve unauthorized access to the user's account from remote station. By flooding packets into the network, the attacker is able to reveal some vulnerability points, consequently using this points to gain authorized access to the network resources. Some of these attacks are: dictionary attacks and FTP_write attack.

D. Probing/scaning attacks

Using network map which contains information about devices and services, the attacker scans network recourses to exploit vulnerability points. The information gained from this attack can be used later to plan more effective attacks. For example, the attacker can perform port scanning to check which points are open, then he will use this ports to perform other attacks.

E. Eavsedropping

In this case, tha attscker who gained an access to the data path can easily "listen" to the data tranffic or even interpret it. This attack is also known as sniffing or snooping.

F. Data modification

After an attacker has gained the access to network's traffic data, another attack is employed which is data modification or altering. The attacker can change the data without sender or receiver notice. This attack can cause big problems to the network user especially when data secrecy is required, as in online marketing.

G. Man in the middle attack

In this attack, all packets exchanged between two users is passes through the compromised device. The attacker could modify the packets without being noticed by the sender or receiver.

III. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion detection systems can be defined as a group of hardware and software mechanisms that tries to prevent actions leading to compromise confidentiality, integrity and availability of network resources [5]. By gathering and analyzing the data flows through the network, IDS can detect potential attacks. Most recent known attacks have signatures which are saved in IDS databases and used to detect these attacks. These databases are modified by human experts whenever new types of attacks appear. IDS are monitoring the network, collecting information then analyzing it to map any detected actions to the previously existing signature which in result contribute to attack detection. Host based IDS (HIDS) and network based IDS (NIDS) are the basic two types of intrusion system classes [6]. While HIDS watches particular host activities like system logs and process activities, NIDS monitor and analyze the whole network's traffic. Many works reported on different host and network based intrusion detection systems, for example in [7] two sensors were implemented together to detect the intrusion. The proposed sensors are either microwave or infra red sensors, the first sensor is used to detect any abnormal action, once the action detected, second sensor is triggered to confirm the intrusion within detection area. In [8] author proposed host based intrusion detection system which detects the unauthorized user attempting to enter into the computer system by comparing user actions with previously built user profile. Rowett et al. [9] proposed to embed the intrusion detection system in different network processing devices. As an example, a reconfigurable semantic processor (RSP)can perform intrusion detection function in multiple network routers, switches and servers which distributed throughout the network. This RSP generates tokens that identify different syntactic elements in data stream than can be associated with any kind of intrusion.

Figure 1. Illustrates the implementation of both NIDS and HIDS to protect the network.

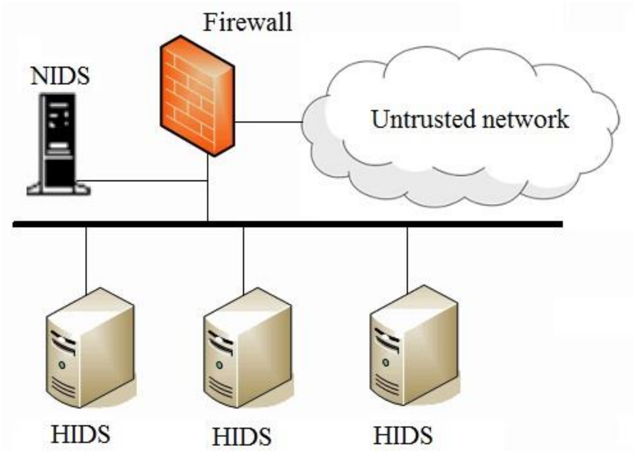

Fig. 1. *Implementation of NIDS and HIDS in computer networks.*

As all intrusion detection systems works by collecting and analyzing networks data to detect the unusual actions, four basic steps can be used to describe intrusion detection systems principle of work, which are[10]:

- Data collection

First of all the data used to determine the intrusions are collected. The useful data contains host processing data, memory and hard disk usage data and system calls data, also network traffic data can be collected using software like TCPDUMP. For host based intrusion detection systems, commands like netstas, strace and ps can be used for this purpose.

- Feature vector creation

As the amount of collected data is huge, it will not be useful until it is filtered to small groups contain only the data that are useful to detect the intrusion. This information groups are called feature vectors. For example, feature vectors for network based IDS can include IP packet headers, which contain source and destination addresses, packet length and transport layer protocol type. For host based systems, it can include user information such as log in time, session duration and files used.

- Data analysis

In this stage, the data collected from both host and network sources are analyzed in order to detect any abnormal activities.

- Reaction

After analyzing the data a decision is made whether the intrusion happened or not. Once the intrusion detected, IDS informs the administrator using different facilities such as email alert or another visualization alerts. Some of intrusion system have an ability to prevent the attacks by controlling network resources, for example, the intrusion detection system can close the opened ports once the attack is detected. The common architectural framework of any intrusion detection system can be illustrated as in Figure 2.

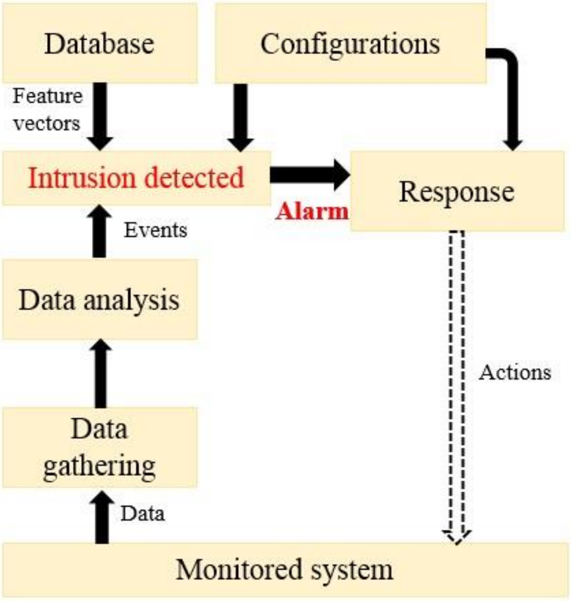

Fig. 2. *Principle of work for intrusion detection systems.*

IV. INTRUSION DETECTION SYSTEMS CLASSIFICATION

Many intrusion detection systems were proposed to provide high level of network security. As different attacks target different network components, each intrusion detection system uses different mechanisms and parameters to detect and prevent the attack. However, all these systems use general framework to detect the intrusion. The general framewark for IDS can be classified into two categories [11, 12]:

A. Misuse or attack signature detection

Each attack is pre-described with some action or group of actions well known to the IDS. By monitoring network activities, IDS are able to define the misbehavior and link it to the specific attack using the information from its database. The main disadvantage of this technique is that every action requires an entry in the database, with thousand actions which can be mapped to every single attack. Furthermore, only attacks which has an entry in the data base can be detected, which means that the system is unable to detect new attacks which will rise in the future.

Two misuse detection techniques are the most famous:

1. **Expression matching based detection:** In this case, the IDS searches in the system entries for occurrence of specific pattern. For example, HTTP request send by the intruder can be matched with log entries to detect the intrusion.
2. **State machine based detection:** A state machine model is built to describe every event sequences. Each event reaches final state which is tagged as “Safe” considered normal, however events which final state is tagged as “Attack” will be considered as intrusion [13]. For each single attack, a model with all possible scenarios should be built, anyway the approach enable the complicated attacks to be easily detected. Reduced number of false alarms is the main advantage of this techniques, furthermore, these systems can easily identify the most proper security tool to be used to prevent the intrusion as attacker background data is already provided. Misuse techniques can detect attacks only that have entries in its data base, in addition, the data base should be updated frequently to include new attacks information. Figure 3. Shows general state machine model used by IDS.

B. Anomaly detection

In anomaly detection case [14, 15], intrusion detection systems try to detect abnormal actions either in host or network. Using this technique, any action which is detected different from the usual legitimate actions is seen as intrusion. A statistical method is normally used in anomaly detection, where the normal user activities is defined first using statistical methods like Hidden Markov Model (HMM), then a group of state transition sequences is generated and saved in system’s database. By monitoring the activities run on the host or network and compare them to the normal activities, any unusual action can be easily detected. Anomaly detection has an advantage over misuse detection such that all known and unknown attacks can be detected with equal efficiency.

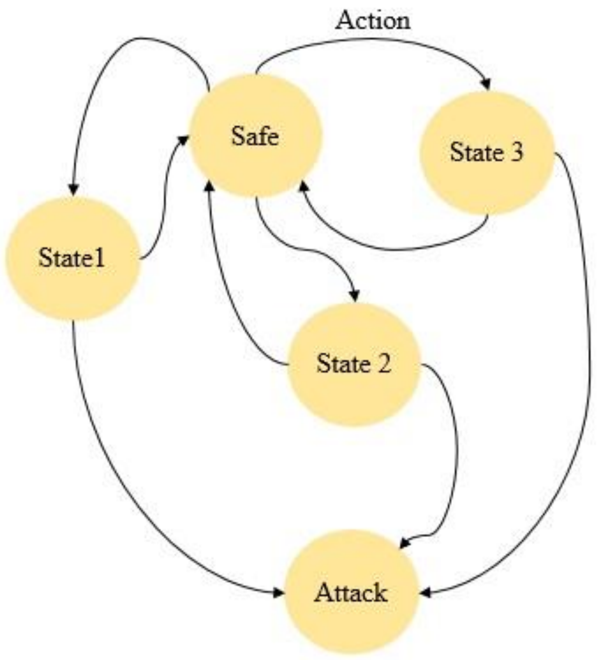

Fig. 3. *Intrusion detection based on state machine action sequences.*

Anomaly detectors are built to detect patterns of behavior which is unusual for the system, and can be considered as intrusion. According to [15], anomaly detection can be classified into static and dynamic.

In static anomaly detection, the parameters monitored by IDS are static. Data files, which can be seen as string of binary code and system codes are examples of static parameters being monitored by static anomaly detection systems. Once a deviation from its original case is detected, the system alerts for intrusion. Thus, static anomaly detectors are said to provide data integrity checking.

In dynamic anomaly detection, the system monitor all the activities and procedures performed be the network. IDS define the sequence of events which is normally repeated and save them in its data base. For example, audit records produced by the operating system OS have strict sequence, and can be done only by the OS. When any other sequence claimed to be done by the OS, the IDS flag it as possible intrusion. The initial events sequence can be associated with some parameters to ease the procedure of comparison, consequently all activities can be traced with high accuracy. For example, the activities can be linked with certain user or certain account to ease tracking process.

Two types of anomaly detection systems are explained here:

1. **Protocol based anomaly detection:** These systems trying to detect any anomaly behavior related to either protocol's format or its procedures [16]. The protocols covered by these detectors include network and transport layer protocols (TCP/IP) as well as application layer protocols. For example, unusual IP defragmentation or TCP reassembly will be seen as anomaly. On the application layer protocols, detectors should be able to perform protocol parsing (decoding). Some of application layer protocol anomalies that can detected contains: illegal field lengths and values, unusual commands use, running certain service/protocol on non-standard port, and illegal number of occurrence of certain commands [17].

2. **Statistical based anomaly detection:** A statistical analysis of the observed objects is used to detect the intrusion [18]. For example, the TCP long-term traffic is observed and analyzed in the absence of the attack to build statistical model. Then short-term traffic is monitored and compared to previous one to detect any possible intrusion. One of the major disadvantages of statistical anomaly detection that it may raise false alarm. The difference between short-term and long-term profiles introduce difference in rare events which will be seen as intrusion. Anyway setting some sensitivity level will be useful to reduce such kind of alarms.

Generally, anomaly detection is advantageous over misuse detection as it can detect the misbehavior without any previous knowledge of the attacker or intruder, furthermore, gathered information could be used to create signature for these attacks. The main disadvantage is increased false alarms due to lack of information about user and environment behavior. Table 1. Shows basic comparison between misuse detection and anomaly detection techniques.

TABLE 1. A COMPARISON BETWEEN MISUSE AND ANOMALY DETECTION TECHNIQUES.

feature	**IDS detection techniques**	
	Misuse detection	***Anomaly detection***
Attacks detected	Known attacks only	Any type
Attack background data required	Yes	No
False alarm rate	Low	High
Need update	Yes	No
Attack type	Defined	Cannot be defined
Protection tool identification	Yes	No

V. RECENT IDS TOOLS

Many intrusion detection tools either host based or network based are commercially available, some of them even license free tools [19-22]. In this section, we introduce most recent IDS tools.

A. *Security Onion*

A tool for network monitoring and intrusion detection. This tool provide good monitoring for virtual LANs and subnets, also it can be configured to act as host based intrusion detector.

B. Ossec

This tool is host based intrusion detection tool and open source. It is compatible with most operating systems including windows and Linux. In addition to intrusion detection, this tool can provide some extra services like file integration checking service and real time rootkit detection.

C. Open WIPS-NG

A wireless intrusion detection and prevention system which depends on servers, sensors and interfaces to achieve security functions. The tool is license free and run using commodity hardware.

D. Snort

Network intrusion detection tool which excels at traffic analysis and packet logging on IP networks [20]. Using content searching and protocol analysis for intrusion signature identification, Snort provide security against worms, vulnerability exploits, port scans and other intrusion attacks.

E. Suricata

This tool compete directly with snort and has the similar structure, even it use same rules to identify the intrusion. Being newer than snort and free available made this tool the most required IDS among all organizations.

VI. CONCLUSION

In this paper, we introduced the basic concepts of intrusion detection systems. As it can be seen, different approaches have different advantages and disadvantages for attacks detection, however, each organization should be able to define the most probable threats for its network. Deep study and analysis of security requirements can lead to better configured security system and hence improved security level. Distributed defense mechanism which involve different types can be implemented to enhance the security, like providing intrusion detection tools for both hosts and networks.

REFERENCES

[1] A. Banathy, G. Panozzo, A. Gordy, J. Senese, ” A Layered Approach to Network Security” 2013, available on line http://www.industrial-ip.org.

[2] Jerry Shenk ,” Layered security: Why it works” , SANS institute publications , 2013.

[3] Sapate, Pritam, and Shital A. Raut. "Survey on classification techniques for intrusion detection”, 2014. available on line http://airccj.org.

[4] J. Rayin, “ A survey of cyber attack detection strategies”, International Journal of Security and Its Applications, vol. 1 No. 1, 2014.

[5] http://technet.microsoft.com/en-us/library/cc959354.

[6] http://insecure.org/stf/secnet_ids/secnet_ids.

[7] J. F. Madox et al. “ Intrusion Detection System “, US Patent, No.4772875, Sept. 1988 .Availableonline http://www.google.com/patents/US6405318.

[8] C. H. Rowland, “Intrusion Detection system”, US Patent, No. 6405318 B1, Jun, 2002. Available online http://www.google.com/patents/US4772875.

[9] K. J. Rowett et al. “ Intrusion detection System", US Patent, No. US2005/0216770 A1, Sept 2005. Available online http://www.google.com/patents/US20050216770.

[10] A. Lazarevic, V. Kumar and J. Srivastava, "Intrusion detection: A survey,” Managing Cyber Threats, US Springer, 2005.

[11] KR, Karthikeyan, and A. Indra. "Intrusion Detection Tools and Techniques–A Survey." 2010. available on line http://www.ijcte.org.

[12] K. Labib, "Computer security and intrusion detection." Crossroads 11, No. 1, 2004.

[13] Gaidhane, Roshani, C. Vaidya, and M. Raghuwanshi. "Survey: Learning Techniques for Intrusion Detection System (IDS)." 2014. Available on line http://csidl.org.

[14] G. Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security journal, elsevier, 2009.

[15] G. Tripp, “A finite-state-machine based string matching system for intrusion detection on high-speed networks”, *EICAR 2005 Conference Proceedings*, 2005.

[16] V. Chandola, A. Banerjee, and V Kumar, “Anomaly Detection: A Survey” 2007. Available on line http://www.cs.umn.edu

[17] Jones, Anita K., and Robert S. Sielken. "Computer system intrusion detection: A survey." Computer Science Technical Report, 2000.

[18] Sekar, R., et al. "Specification-based anomaly detection: a new approach for detecting network intrusions." Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002.

[19] Wang, Ke, and Salvatore J. Stolfo. "Anomalous payload-based network intrusion detection." Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2004.

[20] Ye, Nong, and Qiang Chen. "An anomaly detection technique based on a chi- square statistic for detecting intrusions into information systems." Quality and Reliability Engineering International, 2001.

[21] M. Pascucci,” Top Five Free Enterprise Network Intrusion Detection Tools”, 2014. Available on line http://searchsecurity.techtarget.com.

[22] http://sectools.org/tool/snort.