Intrusion Detection Systems Overview

Chris Figueroa
East Carolina University
figueroac13@ecu.edu

Abstract

Modern intrusion detection systems provide a first line of defense against attackers for organizations. These systems com in various forms and provide both simple and complex functions to facilitate the specific needs of the organization or individual. An overview of intrusion detection systems is provided including the differences between an intrusion detection system and an intrusion prevention system. Several of the intrusion detection methods and techniques such as misuse detection and anomaly detection will be covered. A review of the different types of intrusion detection systems including network-based, client-based, software-based, and appliance-based systems has been included. IDS offerings from several vendors have also been selected and reviewed detailing some of the features of each. Finally, some suggestions and guidelines for selecting the right intrusion detection system for an individual or organization will be provided.

1. Introduction

Computing networks have become the backbone of commerce, communication, and connectivity around the world. Large amounts of sensitive data pass through these networks on a regular basis including personal information and trade secrets. This data in not only valuable to the companies and individuals who create and maintain it, but to those who wish to steal and profit from it as well. In order to prevent such attacks organizations use several methods to secure their networks and data. Intrusion detection systems (IDS) and prevention systems (IPS) along with the firewall are often the first line of defense in preventing cyber attacks. An IDS is software that automates the intrusion detection process [1]. An IPS is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents [1]. These systems come in several forms and varieties using different techniques to detect and prevent cyber attacks. There are many IDS and IPS available on the market today making it important for organizations and individuals to the select what system is best for them. Networks are evolving and cloud computing is becoming the norm for many organization which in turn has raised the need for new types of IDS and IPS in the future.

2. Intrusion Detection

Intrusion detection (ID) is defined as a type of security management system for computers and networks which gathers and analyzes information from various areas within a computer or a network to identify possible security breaches [2]. IDS use several methods in order to detect intrusions however; they are not a complete defense. IDS can provide the following [3]:

a. CAN add a greater degree of integrity to the rest of your infrastructure.
b. CAN trace user activity from point of entry to point of impact.
c. CAN check and report alterations to data.
d. CAN automate the task of monitoring the Internet for the latest attacks.

e. CAN detect when your system is under attack
f. CAN detect errors in your system configuration.
g. Can guide the system administrator in the viral step of establishing a policy for computing assets.
h. CAN make the security management of your system Possible by non-expert staff.

IDS cannot provide the following:

a. CAN NOT compensate for weak identification and authentication mechanisms.
b. CAN NOT conduct investigations of attack without human intervention.
c. CAN NOT compensate for weaknesses in network protocols.
d. CAN Not Compensate for problems in the quality or integrity of information the system provides.
e. CAN NOT analyze all the traffic on a busy network.
f. CAN NOT always deal with problems involving packet-level attacks.
g. CAN NOT Deal with some of the modern network hardware features.

3. Intrusion Prevention

Intrusion prevention (IP) is defined as a preemptive approach to network security used to identify potential threats and respond to them swiftly [4]. An IPS detects intrusions similar to and IDS however, an IPS takes immediate action on what is detected as a threat. These actions can include dropping a packet that is determined to be malicious or completely block traffic from a malicious source and are based on parameters set by the systems administrator. Today IDS and IPS are often combined into one system offering detection and prevention in one package.

4. Intrusion Detection Methods & Techniques

The goal of intrusion detection is to identify possible attacks by analyzing data or network traffic. However, there are several methods of ID which can be used to accomplish this task, the IDS may use one or several of them depending on the system being used. The methods of intrusion detection which can be used include misuse detection, anomaly detection, specification based detection, and hybrid detections. Within each of these methods of ID are several techniques which are used to identify threats.

4.1 Misuse Detection

Misuse detection is used in detecting known attacks by matching gathered information to a database of attack signatures. This method of ID is only as good as the database of signatures that it has access to and will not detect any new or undocumented attacks. Four classes of techniques are commonly used to implement misuse detection, namely pattern matching, rule-based techniques, state-based techniques and data mining [4].

4.1.1 Pattern Matching

Pattern matching uses reads the data in a packet and looks for a fixed sequence which is often associated with a service and source or destination port. Newman [5] states that many protocols and attacks do not make use of well-known ports, and pattern matching thus has difficulty detecting these kinds of attacks. In addition, pattern matching can result in many false positives if the pattern is not extremely unique.

4.1.2 Rule Based Techniques

Rule based pattern matching techniques use expert systems which match gathered data or network traffic with scenarios based on rule sets. These types of expert systems are often forward-chaining systems which can deduce new facts based on existing facts. Within an intrusion detection system, event records are asserted as facts and evaluated against penetration rule sets. As individual rules are evaluated against facts and satisfied, the individual event records provide a trail of reasoning that allows the user to analyze the evidence of malicious activity in isolation from the full event stream [6]. In order for rule-based techniques to be successful the security officer will have to continuously add rules as new attacks and scenarios are discovered.

2.1.3 State-Based Techniques

According to Ghorbani [4] state-based techniques detect known intrusions by using expressions of the system state and state transitions. In state-based techniques the state of the system is dictated by the users and processes affecting the system. The system will start at an initial state and will be in a transitional state until an attack is completed which will then trigger the alert. These states can be represented by using a state transition diagram (fig. 4.1).

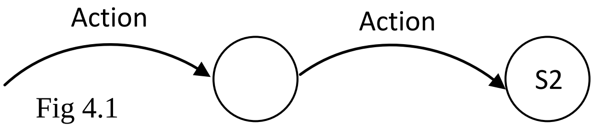

Fig 4.1

The initial action begins the penetration scenario resulting in a new state and when the ends when the system is in a compromised state.

4.1.4 Data Mining

Data Mining involves searching through large amounts of information looking for patterns using a specific set of rules. In regards to ID, data mining can be used to identify attacks by using gathered network data and baselines. In addition, data mining can be used to detect false alarms as it will use historical data to trigger events. There are several data mining techniques which can be used in and IDS including offline and real-time processing both of which have their positives and negatives. The use of multiple sensors to collect data by various sources has also been presented by numerous researchers as a way to increase the performance of an IDS [7]. Data mining is good for detecting known attacks however, performs poorly when in detecting new attacks.

4.2 Anomaly Detection

Where misuse detection looks for patterns and known attacks, anomaly detection attempts to identify differences in normal operations in order to detect an intrusion. This is done by first establishing a baseline of normal activity within the system. Once the baseline data is collected any activity the system deems unusual can then trigger an alarm. However, anomaly detection can lead to many false positives. In order to "teach" the system to recognize normal activity, several methods can be used including advanced statistical models, rule based techniques, biological models, and learning models.

4.2.1 Advanced Statistical Models

Advanced statistical models use complex statistical algorithms to created a baseline and look for anomalies. There are several models which use metrics such as

CPU cycles, the number of files opened, and which machines users have logged into. All packets are given an anomaly score (indicating the degree of irregularity for the specific event) and if the anomaly score is higher than a certain threshold, the IDS will generate an alert [8].

4.2.2 Rule Based Techniques

There are several rule based techniques which could be used for anomaly detection. Most of which include the use of expert systems to gather information based on a rule set which is then analyzed and compared to the baseline data that has been generated.

4.2.3 Biological Models

Biological models use systems found in nature as the basis of their functionality. For example, Cai [9] proposes an anomaly detection system based on biological immune systems. These systems attempt to treat intrusions as foreign objects to the system and produces an alarm when is found.

4.2.4 Learning Models

Similar to biological models, learning models attempt to mimic the biological process of learning. Some of these models are based on neural networks which simulate the work of neurons in the human brain. These neural networks are able to work with imprecise and incomplete data [10]. This allows the system to detect both documented and new attacks. These techniques allow the system to perform anomaly detection unsupervised at it can learn and adapt to new attacks.

4.3 Specification-Based Detection

Specification-based detection approaches are neither misuse based, nor anomaly based since they use system behavioral specifications to detect attacks and premise that every well-behaved system execution shall conform to the specification of its intended behavior [4]. This form of detection uses specifications which the system must then use. If there is any deviation from these specifications then it is considered an attack and an alarm is raised. Supporting current operating methods with specifications-based detection is difficult as specifications would have to be defined for each program.

4.4 Hybrid Detection

Hybrid detection used both misuse and anomaly detection methods. Misuse detection is used in order to identify known attacks while anomaly detection methods are used to indentify unknown attacks. These systems attempt to minimize the negatives of each both methods and leverage their advantages.

5. Intrusion Detection Approaches

IDS use can use different approaches in detecting attacks. These include a host-based approach which is run on each individual machine on the network and the network-based approach which is run on a server or network appliance. In addition some IDS use a hybrid approach taking advantage of both methods.

5.1 Host-based IDS

Host-based IDS are run on each machine in the network and use the log files to search for the attack signatures. Because the host-based IDS protects the server "at the source," it can more intensely protect that specific computer [11]. Host-based IDS can also use port monitoring to identify any possible attacks. This type of IDS is software based as it must be installed on the host machine.

5.2 Network-Based IDS

Network-based IDS monitors the data on the network as well as from individual machines. The IDS then examines each packet in order to determine if an attack is occurring. There are three types of signatures which the IDS looks for including string signatures, port signatures, and header condition signatures.

5.2.1 String Signatures

String signatures look for a string which could be part of a possible attack. However, using this type of signature could lead to many false positives. To refine the string signature to reduce the number of false positives, it may be necessary to use a compound string signature [12].

5.2.2 Port Signatures

Port signatures monitor connection attempts on well known ports. Some of these ports include telnet (TCP port 23) and FTP (TCP ports 20/21). If there are ports being used which are not normally used by the system the IDS detects this as an attack.

5.2.3 Header Condition Signatures

Header condition signatures look for dangerous or illogical combinations in packet headers [13]. An example of this type of signature is a TCP packet with both the SYN and FIN flags set, notifying the system that a connection is to be started and stopped at the same time.

5.3 Hybrid IDS

A Hybrid IDS uses both host-based and network-based methods in order to protect the network. By combing both methods the hybrid IDS is able to create a more secure network by monitoring both network traffic and each individual host.

5.4 Software Based IDS

IDS software can either be network-based where it is installed on a central server or on individual client machines running a standard operating system. Using a software based IDS allows administrators to select the hardware onto it will be installed. This can help save on cost as the IDS can be installed on an existing host. In addition, there are free open source software based IDS which are available.

5.5 Appliance Based IDS

Appliance based IDS are hardware which comes with the software already installed. IDS appliances offer "plug and play" setup and functionality with an easier learning curve [11]. These appliances are optimized to run the IDS therefore offer higher performance than a software based solution. In addition, IDS based appliances use proprietary operating systems which are more secure. The cost of an appliance IDS may be less than the cost of IDS software, hardware, and operating system combined.

6. Where IDS Fits

An IDS can be placed on in several configurations within a network. These configurations can include between the edge and back-end firewall, in front of the edge firewall, and behind the back-end firewall.

6.1 Between the Edge and Back-end Firewall

Placing the IDS between the edge firewall and the back-end firewall in the demilitarized zone (DMZ)(Fig 6.1) will allow the firewall to block most attacks and let the IDS detect those that make it through. This type of configuration is network based and will detect attacks from external sources but cannot detect those from internal ones.

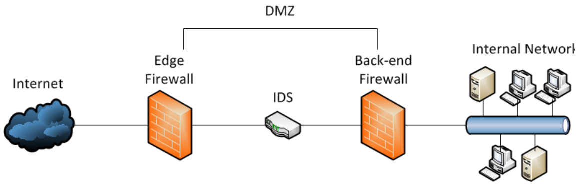

Fig 6.1

6.2 In Front of the Edge Firewall

Placing the IDS in front of the edge firewall (Fig 6.2) will all it to catch any attacks from external sources targeted at the network and is network-based. However, the IDS will detect many attacks which could have been blocked by the edge firewall.

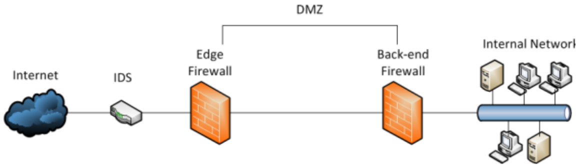

Fig 6.2

6.3 Behind the Back-End Firewall

Placing and IDS behind the back-end will detect and attacks from internal sources. This type of configuration often includes an additional IDS located within the DMZ (Fig 6.3) to detect any attacks from external sources. This configuration can be a mix of network and client based IDS.

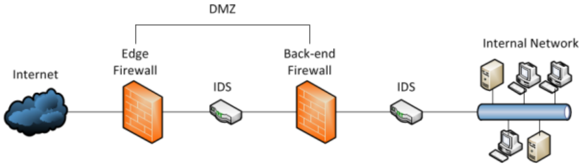

Fig 6.3

7. Available IDS Solutions

There are many available IDS solutions on the market today ranging from simple client-based system to complex network-based appliances. The cost of these IDS can range anywhere from free and open source to thousands of dollars. The following is an examination of some of the more popular available IDS solutions.

7.1 Snort

Snort is a free open source software-based IDS developed by Sourcefire. Snort is a network based IDS and offers signature, protocol, and anomaly based inspection. In addition, the Snort IDS provides the real time analysis of IP packets and has the capability of performing port scans. Sourcefire also offers a commercial product based on the Snort engine for businesses.

7.2 GFI LANGuard S.I.M

GFI LANGuard System Integrity Monitor (S.I.M.) is a free client-based IDS. GFI LANGuard S.I.M. is a utility that provides intrusion detection by checking whether files have been changed, added or deleted on a system [13].

7.4 GFI LANGuard

The premium version of GFILanguard offers more features than the free version and is geared towards businesses. The IDS is network based and can perform port monitoring. Furthermore, GFI LANGuard also offers vulnerability assessment and patch management features.

7.5 Proventia IDS

The Proventia is an appliance based solution that offers both IPS and IDS capabilities. Due to its cost the Proventia is geared toward medium to large businesses. The software on the appliance is based on RealSecure and is designed for aggregate network bandwidths of 200Mbps to 1200Mbps.

7.6 Cisco Secure IDS

The Cisco Secure IDS is another appliance based solution aimed at medium to large businesses. This IDS uses stateful pattern recognition, heuristic detection and anomaly detection. Models are available to handle traffic from 80Mbps to 1000Mbps.

8. Selecting an Intrusion Detection System

Intrusion detection is important for any network and selecting an IDS from all of the available solutions can be daunting. For small business or home networks a low cost or open source solution would be ideal. However, for medium to large businesses there is more to take into account. Bunocore [14] suggest that businesses consider the following when selecting an IDS:

1. Identify the need

2. Gain a general understanding of intrusion detection systems

3. Gain a detailed understanding of the network

4. Evaluate various IDS systems

5. Determine Policy and procedures

Using these considerations companies can decide whether a software-based or appliance-based solution is the correct fit for their network and how much money they are willing to spend on the security of their data.

9. Conclusion

Intrusion detection is an important facet of network security to both small and large organizations. There are several methods available for detecting threats and can be combined in order to provide improved protection. IDS can be either network-based or client-based an offer protection to varying degrees. There are several vendors which offer solutions that range from free and open source software-based solutions to network appliances which can cost thousands of dollars. Selecting the best one for a specific network can be a daunting task but, by identifying the needs of the business and understanding the network will make the process more manageable for administrators.

10. References

*[1] I. Mukhopadhyay, M. Chakrabory, and S. Chakrabarti, “A comparative study of related technologies of intrusion detection & prevention systems,” Journal of Information Security, 2011,2,28-38.

[2] M. Rouse, “Definition of intrusion detection”http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection, accessed, March, 2014.

*[3] B.M. Beigh, Prof. M.A.Peer, “Intrusion detection and prevention system: Classification and quick review” ARPN Journal of Science and Technology, 2012, 2,7, 661-675.

*[4] A.A. Chorbani, W. Lu, M. Tavallaee, "Network intrusion detection and prevention:

Concepts and Techniques" http://link.springer.com.jproxy.lib.ecu.edu /book/10.1007/978-0-387-88771-5 accessed March, 2014.

[5] D. newman, K.M. Manalo, E. Tittel, "Intrusion detection overview" http://www.pearsonitcertification.com /articles/article.aspx?p=174342, June, 2004.

*[6] U. Lindqvist, P.A. Porras, "Detecting computer and network misuse through the production-based expert system toolset (P-BEST)" Proceedings of the 1999 IEEE Symposium on Security and Privacy, May, 1999

[7] T. Lappas, K. Pelechrinis, "Data mining techniques for (network) intrusion detection systems" http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDsQFjAA&url=http%3A%2F%2Ftrac.assembla.com%2FodinIDS%2Fexport%2F12%2FEgio%2Fartigos%2Fdatamining%2FdataIDS.pdf&ei=fRdAU8HSCsuysQSFn4DwDw&usg=AFQjCNFDvhoyd9_O3hDkPyskq3OI-R2ANQ&sig2=tvhv1ucpzYUEuNvdXCtY6Q, Accessed April, 2014.

[8] J. Farshchi, "Statistical-based intrusion detection", http://www.symantec.com/connect/articles/statistical-based-intrusion-detection, April, 2015

*[9] M. Cai, "A novel immunity-based model for anomaly deteciton" 2008 International Conference on Computer Science and Software Engineering, 2008.

[10] P. Kukielka, Z. Kotulski, "Adaptation of the neural network-based IDS to new attacks detection", http://arxiv.org/ftp/arxiv/papers/1009/1009.2406.pdf, Accessed March, 2014.

[11] D. Shinder, " SolutionBase: understanding how an intrusion detection system (IDS) works, http://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/, July, 2005.

[12] S. Northcutt, "Intrusion detection FAQ: what is network intrusion detection?" http://www.sans.org/security-resources/idfaq/network_based.php, Accessed April, 2014

[13] gfi.com, "Introduction to LANGuard S.I.M.", http://support.gfi.com/manuals/en/lansim/introductiontolanguards.i.m..htm, Accessed April, 2014.

[14] SANS Institute, "Selecting an intrusion detection system", https://www.sans.org/reading-room/whitepapers/detection/selecting-intrusion-detection-system-338, Accessed April, 2014.