ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2014,
Vol. 7, No. (3):
Pgs. 344-350

Improving Network Attack Alarm System: A Proposed Hybrid Intrusion Detection System Model

OJEME BLESSING ONUWA

Mathematics and Computer Science Department, Delta State University, Abraka.

(Received: November 05, 2014; Accepted: December 10, 2014)

ABSTRACT

Intrusion Detection System (IDS) serves as an important tool in preventing, detecting and defending against network attack. Due to increasing incidence of cyber-attacks, building an effective hybrid intrusion detection system is essential for prevention of any attack, protecting information system, monitoring networks against attacks or intrusion, and reporting these attacks to the appropriate centre for immediate action. In this paper, a hybrid intrusion detection system, integrating the strengths of the misuse detection system and the anomaly detection system were used to reduce the chances or occurrence of attacks on the network to a minimal level. This system works as an alert device in the event of attacks directed at an entire network and it also helps in reducing the number of false positive as well as false negative alarm.

Key words: Networks, Alarm system, Hybrid.

INTRODUCTION

Since the invention and advancement in technology, people have been finding ways of attacking the network through the development of software and other malicious acts. Over the past few years, these attacks have increased to the point where almost every computer and network is exposed to some form of attack. It might come as a shock to many that as we strive hard throughout the day working up to about ten hours daily in order to secure the network from attacks, the same way an attacker spends all day modifying network attack techniques and looking for networks to exploit. The environment is constantly evolving and changing fields by new technology and the internet (Meera and Srivatsa, 2011). Awareness of these network attacks and ways of preventing them helps in managing threats and vulnerability in this changing environment. These threats may be a curious person, an angry employee, espionage from a rival company or a foreign government (Biermann and Cloete, 2001). There are many research works published on various ways of preventing and protecting computer networks from malicious attacks. This paper creates a hybrid model that equips users with the expertise to prevent and checkmate these attacks to certain degrees.

Related Literature

One of the most effective and efficient security mechanisms for checkmating the activities of an attacker on the network and protect the network against malicious attacks or unauthorized access is the Intrusion Detection System (Hichem and Mohamed, 2011). This mechanism, usually considered as a second line of defense, can protect with high accuracy against internal attacks. It allows detecting abnormal or suspicious activities on the analyzed target and triggers an alarm when intrusion occurs.

Two techniques mainly used for intrusion detection are Misuse Detection and Anomaly Detection (Kumar, 1995; Wassim et al 2008). Misuse Detection technique involves the comparisons between captured data and known attack signatures, where any corresponding pattern can be considered as an intrusion (Jawhar and Mehrotra, 2010). Updating the signature over time is necessary to keep this technique effective. However, the major drawback of misuse detection systems is its inability to detect new security attacks that were not published (Kaplantzis, 2006; Jawhar and Mehrotra, 2010). Anomaly Detection technique is based on modelling the normal behaviour of the nodes and compare the captured data with this model. Any activity that deviates from this model can be seen as anomaly (Prabhdeep and Vashisht 2013). The advantage of such technique is that it can detect new security attacks but requires a considerable computational time for extensive training of data for artificial learning algorithms. Again, anomaly-based technique may cause a significant number of false alarms because the normal behaviour varies widely and obtaining complete description of normal behaviour is often difficult (Kaplantzis, 2006). To overcome the individual limitations of the above two techniques, a hybrid model comprising the combination of the synergistic advantages of the misuse and anomaly detection systems is proposed.

Halme and Bauer (1995) have identified intrusion detection as one of six components in their taxonomy of anti-intrusion techniques. The first three components which they identified; prevention, preemption and deterrence, are primarily based on passive measures which decreases the likelihood of a successful attack on a system. These components address the policy related issues of information security and those elements which can be incorporated into a system with minimal effort. Examples of these include the establishment of organizational security guidelines, security education and training, and the posting of warning notices on the initial screen of a system. The last three components, deflection, detection and countermeasures are more active measures designed to protect the critical element of a system. Then accurate detection of a system intrusion is the most critical of the six components. While additional measures may be very effective at preventing an eventual penetration of the system, all security measures rely on the accurate identification of an attack prior to the employment of defensive measures.

Intrusion Detection System (IDS)

A network Intrusion Detection System (IDS) is used to monitor networks for attacks or intrusion (Meera and Srivatsa, 2011). A large network intrusion detection system server can be set on a backbone network, to monitor all traffic; or smaller systems can be up to monitor traffic for a particular server, switch, gateway, or router (Meera and Srivatsa, 2011).

A network could be used to send the attack (such as a worm), or it could be the medium of attack (Denial of Service) attack. However, there are several types of network attacks that do not attack computers, but rather the network they are attached to. Flooding a network with packets does not attack an individual computer, but clogs up to the network. Although a computer may be used to initiate the attack, both the target and the means of attacking the target are network related. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable. When deployed, intrusion detection complements these protective mechanisms to improve the system security (Amrita and Brajesh, 2012). The diagram below shows the various states of security system.

The attack process

The attack can be launched in times of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packets or connection within a few seconds (Faizal et al, 2010). Meanwhile, slow attack refers to an attack that takes a few minutes or a few hours to complete (Faizal et al, 2010). Both of the attack gives a great impact to the network environment due to the security breach decade (Amrita and Brajesh, 2012). There several distinct stages that makes up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four (4) main stages:

- Attacker motivation and objectives
- Information gathering/Target selection
- Attack selection
- Attack execution

Types of attacks

There are different types of attack that affect the network, and each of these attacks has its aim or objectives for attacking the network. Some attack alters system resources or affect their operation thereby compromising integrity or availability while others attempts to learn or make use of information from the system but does not affect system resources thereby compromising confidentiality. These attacks include:-

Denial of Service (DOS)

One of the major threats to network security is the Denial of Service (DOS) attack. A Denial of Service attack is an attempt to make a computer resource unavailable to its intended users (Meera and Sriatsa, 2011). Not only are DOS attacks easy to execute (Amrita and Brajesh, 2012), but it's among the most difficult to eliminate. For example, one can launch a DOS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim (Amrita and Brajesh, 2012).v an increasingly common attackers tool that has gained widespread public attention is the computer service saturator. A Denial of Service attack is characterized by an explicit attempt by attackers to prevent legitimate user of a service from using that service. Examples include flooding a network, thereby preventing legitimate network traffic and disrupting service to a specific system or process.

Probing/scanning Attack

Probing attack is a class of attack were an attacker scans a network to gather or assimilate information about the system being attacked. Using scanning techniques, the attacker can gain topology information, types of network traffic allowed through a firewall, active hosts on a network, operating system and the kernel of the hosts o the network, server software running, version number of software, etc. (Amrita and Brajesh, 2012). Using this information, the attacker may launch attacks aimed at more specific exploits. The first method of scanning a host is to send a PING request through TCP packet using Internet Control Message Protocol (ICMP) (Simon and Olumide, 2013). ICMP

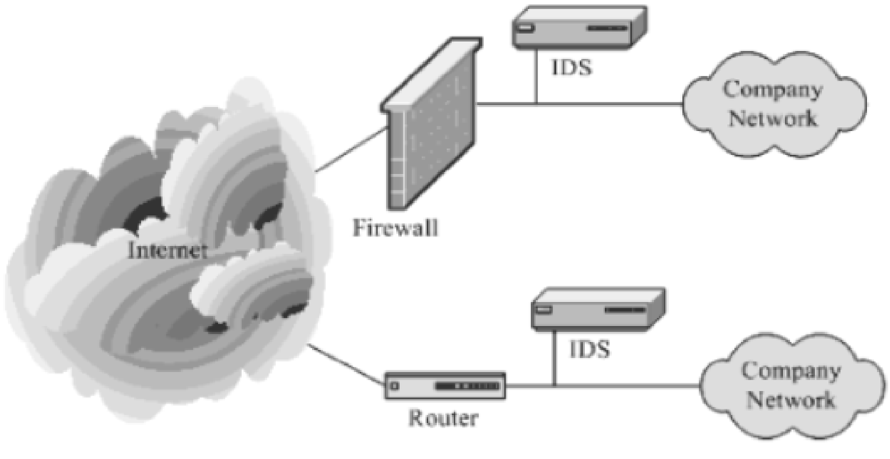

Fig. 1: Intrusion Detection System (Amrita and Brajesh, 2012)

is a protocol within the TCP protocol that allows for normal routing control. A PING Packet will echo through the network and be replied by the host addressed in the packet. PING is a useful tool to determine if a machine is actively on the internet, disconnected or off. But it also allows an attacker to determine if the machine is on and thereby narrow his list of possible targets from all network addresses to only active hosts. This means that firewalls can block ICMP packets to protected systems. The PING scan reveals only limited information, whether the network hosts is on or off, making it one of the least effective scans an attacker can use. The PING scan can be blocked by a firewall, but because detecting if a network host is active is a useful operation for normal network operation, this tends to degrade the normal operation of the network. Still, many network firewalls block PING packets to attempt to protect their systems from PING scan (Simon and Olumide, 2013). Probing attacks involves discovering the algorithms and parameters of the recommender system itself (Iftikhar et al., 2009). It may be necessary for an intruder to acquire this knowledge through interaction with the system itself.

Iftikhar et al., (2009) identified the various types of probing attacks:-

- Ipsweep:- It probes the network to discover available services on the network. First intruder find out a machine on which he may be attacked.
- Portsweep: - It probes a host to find available services on that host. If a service is known on the system so it may easily be attacked by the network intruder.
- Nmap: - It is a complete and flexible tool for scanning a network either randomly or sequentially. Therefore, often intruders used this tool for scanning network parameters that may help them in attacking the system.

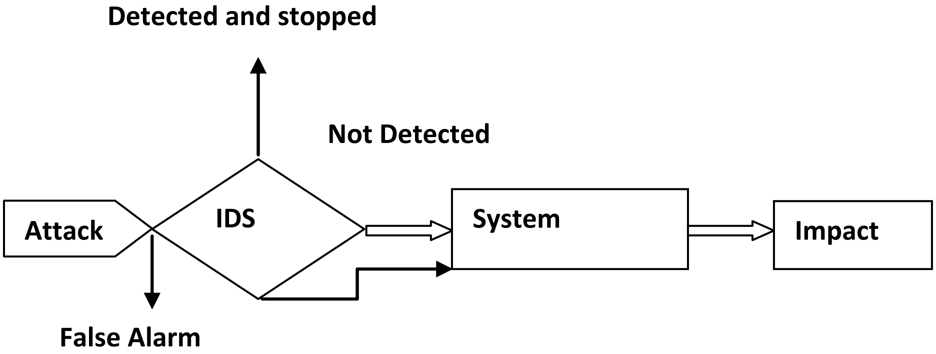

Fig. 2: States of Security System (Tarun *et al.*, 2008)

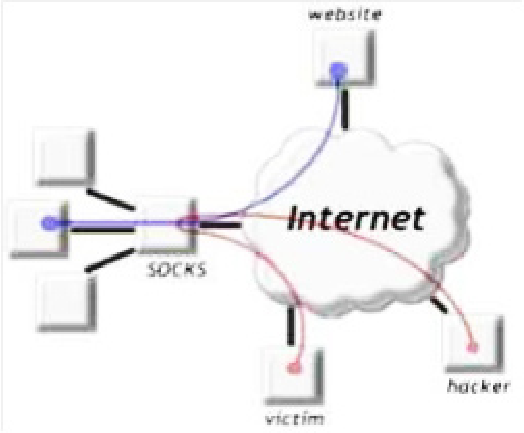

Fig. 3: PortScan (Simon and Olumide, 2013)

- Satan: - It is an administration tool; it gathers information about the network.

Intrusion Detection System (IDS)

The first major work in the area of Intrusion Detection System was discussed by J.P Anderson in 1980. Anderson introduced the concept that certain types of threat to the security of computer system could be identified through a review of information contained in the system's audit trail. Many types of operating systems, particularly the various "flavours" of UNIX, automatically create a report which details the activities occurring in the system. Dr. Dorothy Denning proposed an intrusion detection model in 1987 which became a landmark in the research in this area. The model which she proposed forms the fundamental core of most intrusion detection system methodologies in use today.

METHODOLOGY

Intrusion Detection System is classified into two (2) categories as earlier discussed namely misuse detection (knowledge-based) and anomaly detection (behaviour-based). In this research work, we will be implementing both categories in order to establish a defense- in- depth intrusion detection framework.

Anomaly Detection

The anomaly based system builds a model of the normal behaviour of the system and then looks for anomalous activity such as activities that do not conform to the established model (Amrita and Brajesh, 2012). Anything that does not correspond to the system profile is flagged as intrusion. False alarms generated both systems are major concern and it is identified as a key issue and the case of delay to further implementation of reactive intrusion detection system (Amrita and Brajesh, 2012).

Although, false alarm is a major concern in developing the intrusion detection system especially the anomaly-based intrusion detection system, yet the system has fully met the organizational objectives compared to the signature-based system, that is, misuse system (Garuba et al., 2008). Since pretending to be an authorized user a very powerful method for an attacker to gain access to the system resources, this type of approach looks for the variation in behaviour which might indicate a masquerade.

Misusedetection

A signature-based intrusion detection system also known as misuse or knowledge-based will monitor packets on the network and compare them against a database of signatures (Amrita and Brajesh, 2012) or attributes from a known malicious threats. A signature based intrusion detection system operates in much the same way as a virus scanner, by searching for known attack or signature for each specific intrusion event (Meera and Sriatsa, 2011). And while signature IDS is very efficient at sniffing out known attacks, it does like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker techniques (Meera and Sriatsa, 2011).

This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new types are discovered (Amrita and Brajesh, 2012). Hence, unknown attacks in network intrusion pattern and characteristic might not be captured using this technique (Amrita and Brajesh, 2012). The disadvantage associated with approach occurs when updates are not gotten regularly on new attacker's strategies and also the increase in CPU load for the system when this updates are gotten (Meera and Sriatsa, 2011).

The diagram below explains the integration of both the anomaly based system and the misuse or knowledge based system (combined architecture) in a network traffic situation.

Database: The database contains known attack signatures. Packets from traffic are usually compared

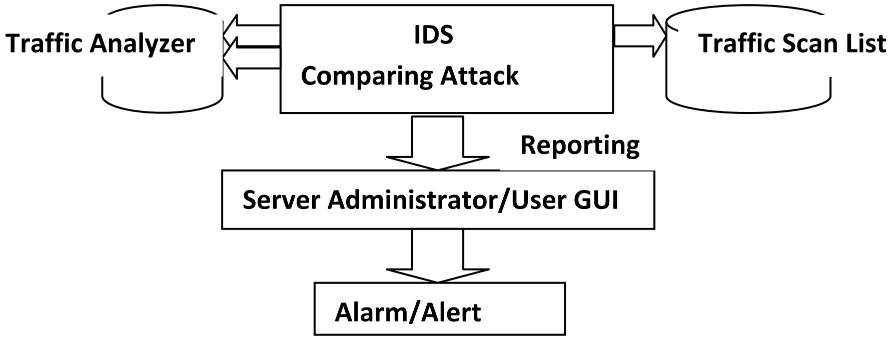

Fig. 4: Model for detecting/preventing Network Attack

with already existing method of attacks.

Model: The model contains profile of monitored activities. This models are usually developed by the administrator based on certain constrains or conditions.

Packet Sniffer: It checks for malicious packets entering the network.

Network traffic coming into the network are being trapped by the packet sniffer installed at the end of the system in a network on which the traffic has to be captured. The packet sniffer detects attacks and treats them as appropriate while attacks not detected are allowed into the Intrusion Detection System. The IDS contains two mechanisms which are the database where known attacks are stored and a model designed by the administrator specifying certain constrains/ conditions. The undetected attacks is sent to the model to check if it meets the constrains or conditions set by the administrator. Any information that does not meet the condition is considered as intrusion be it an attack or not. Suppose the information meets the conditions, it is then passed to the database as the final litmus test were it compared with known attacks before allowed into the system. Although this approach seems to be efficient, its computational time is greatly increased and it requires high storage capacity.

Research has been conducted into intrusion detection methodologies which combine the anomaly detection approach and the misuse detection approach (Lunt, 1989). These techniques seek to incorporate the benefits of both standard approaches to intrusion detection system to monitor for indications of external and internal attacks (Hichem and Mohamed, 2011)

CONCLUSION

Network security is an important field that has is increasingly gaining widespread attention as them internet expands. In this paper work, we have presented an overview of the Intrusion Detection System (IDS) as a mechanism for checkmating network attacks and the types of attacks that are most likely to be associated with the network. A hybrid model for Intrusion Detection System; integrating the misuse or signature based system and the anomaly or behaviour based system was utilized in other to establish a more efficient and effective intrusion detection framework. The major limitations of this model is that it increases the computational time in detecting attacks, it requires large storage memory and implementation of this model using various techniques is expensive. Finally, network attack cannot be totally eradicated because the most serious threats to the integrity and authenticity of computer information come from those who have been entrusted with usage privileges and yet commit computer fraud.

REFERENCES

1. Amrita, A. and Brajesh, P. An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),* **2**(8); 94-98 (2012).
2. Bierrmann, E., Cloete, E. and Venter, L.M. A Comparison of Intrusion Detection Systems, Computers and Security, pp 678-683 (2001).
3. Cabrera, J.B.D, Ravichandran, B. and Mehra, R.K. Statistical Traffic Modeling for Network Intrusion Detection.In proceeding of the IEEE Conference (2002).
4. Cuppen, F. and Miege, A. Alert Correlation in a Cooperative Intrusion Protection framework. In Proceeding of the 2002 IEEE Symposium on security and privacy (2002).
5. Faizal, M.A., Mohd Z.M., Shahrin, S.R., Siti, R.S. and Asrul, H.Y. Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System, Second International Conference on Network Applications, Protocols and Services, IEEE (2010).
6. Garuba, M., Liu, C. and Fraites, D. Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of

fifth International Conference on Information Technology: New Generation, IEEE (2008).

7. Halme, L.R. and Bauer, R.K. A Taxonomy of Anti-intrusion Techniques, Proceedings of the 18th National Information Systems Security Baltimore,MD (1995).
8. Hichem, S. and Mohamed, F. Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network, *International Journal of Network Security & Its Application* (IJNSA), **3**(4), pp1-14 (2011).
9. Iftikhar, A., Azween, B.A., and Abdullah, S.A. Application of Artificial Neural Network in Detection of Probing Attacks, In Proceeding of the 2009 IEEE Symposium on Industrial Electronic and Applications (ISIEA), pp. 557-562 (2009).
10. Jawhar ,M. M. T. and M. Mehrotra, Design Network Intrusion Detection System Using Hybrid Fuzzy-Neural Network. *International Journal of Computer Science and Security*, **4**(3), 285 (2010).
11. Jim, M. Pentagon Expands Cyber-Attack Capabilities, Newspaper Publication, USA TODAY NEWS (2013).
12. Kaplantziz, S. Security Models for Wireless Sensor Network, PhD Conversion Report, Centre of Telecommunications and Information Engineering, Monash University, Australia (2006).
13. Kumar, S. Classification and Detection of Computer Intrusions, PhD Thesis, Department of Computer Science, Purdue University, USA (1995).
14. Lunt, T.F. Real- Time Intrusion Detection. Proceedings from IEEE COMPCON (1980).
15. Meera, G. and Srivatsa, S.K. Detecting and Preventing Attacks using Network Intrusion Detection System, *International Journal of Computer Science and Security,* **2** (1); 49-59.
16. Prabhdeep Kaur, Sheveta Vashisht. Mingle Intrusion Detection System Using Fuzzy, (2013).
17. Logic. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, **2**(3).
18. Simon, E.Y. and Olumide, L. Hybrid Spread-Spectrum TCP for Combating Fraudulent Cyber Activities against Reconnaissance Attacks, *African Journal of Computer Science,* 5(2); 36-48 (2013).
19. Wassim El-Hajj, Fadi Aloul and Zouheir Trabelsi (2008). On Detecting Port Scanning using Fuzzy Based Intrusion Detection System. Wireless Communications and Mobile Computing Conference, IWCMC '08, IEEE press, pp 105-110